ESTUDIO Y PRÁCTICAS SOBRE REDES PRIVADAS VIRTUALES (VLAN y VPN) PARA LOS LABORATORIOS DE LA CUTB

TANIA MARGARITA TORRES MARTÍNEZ

YEZID CHARTUNI CASTRO

Trabajo de Monografía presentado como requisito para aprobar el Minor en Comunicación y Redes.

Director

FRANCISCO JIMÉNEZ CASTILLA

Ingeniero Electrónico

CORPORACIÓN UNIVERSITARIA TECNOLÓGICA DE BOLÍVAR

FACULTAD DE INGENIERÍA DE SISTEMAS

CARTAGENA

2003

Cartagena de Indias, 26 de Mayo del 2003

Señores

CORPORACIÓN UNIVERSITARIA TECNOLÓGICA DE BOLÍVAR

ATTE. : Comité de evaluación de Proyectos

Facultad de Ingeniería de Sistemas

La Ciudad

Respetados señores:

Con la presente me permito dar a conocer mi aceptación como Director de la Monografía: "**ESTUDIO Y PRÁCTICAS SOBRE REDES PRIVADAS VIRTUALES (VLAN y VPN) PARA LOS LABORATORIOS DE LA CUTB**".

Agradeciendo la atención prestada.

Atentamente,

Francisco Jiménez Castilla

Ingeniero Electrónico ----------

Cartagena de Indias, 26 de Mayo del 2003

Señores

CORPORACIÓN UNIVERSITARIA TECNOLÓGICA DE BOLÍVAR

Atte: Comité de evaluación de Proyectos

Facultad de Ingeniería de Sistemas

La Ciudad

Respetados señores:

Con la presente nos permitimos presentar para su estudio, consideración y aprobación, de nuestra Monografía "**ESTUDIO Y PRÁCTICAS SOBRE REDES PRIVADAS VIRTUALES (VLAN y VPN) PARA LOS LABORATORIOS DE LA CUTB**", para aprobar el Minor en Comunicaciones y Redes.

Agradecemos de antemano la atención prestada.

Atentamente,

Tania Margarita Torres Martínez

Yezid Chartuni Castro

ESTUDIO Y PRÁCTICAS SOBRE REDES PRIVADAS VIRTUALES (VLAN y VPN) PARA LOS LABORATORIOS DE LA CUTB

TANIA MARGARITA TORRES MARTÍNEZ

YEZID CHARTUNI CASTRO

CORPORACIÓN UNIVERSITARIA TECNOLÓGICA DE BOLÍVAR

FACULTAD DE INGENIERÍA DE SISTEMAS

CARTAGENA DE INDIAS

2003

Nota de aceptación

Firma de presidente del jurado

Firma del Jurado

Firma del jurado

Ciudad y Fecha

A Dios por darme la vida y la fortaleza para cumplir mis metas, a mis padres por apoyarme en todo momento y a mi esposo por darme aliento en cada dificultad.

Tania Torres Martínez

A Dios por cuidarme cuando he cometido errores y darme la voluntad para cumplir uno de mis objetivos, a mis padres y hermanos por su apoyo incondicional y hacer posible este gran sueño.

Yezid Chartuni Castro

TABLA DE CONTENIDO

INTRODUCCIÓN

Existen dos clases de redes privadas virtuales: V-LAN para enlaces LAN y VPN.

Las V-LAN se basan en el empleo de Switches permitiendo un control más inteligente del tráfico de la red, para que la eficiencia de la red entera se incremente en ancho de banda.

Las LAN virtuales (V-LANs) comunican entre sí como si estuvieran conectadas al mismo concentrador, aunque se encuentren situadas en segmentos diferentes de una red de edificio o de campus. Es decir, la red virtual es la tecnología que permite separar la visión lógica de la red de su estructura física.

Una Red Privada Virtual (VPN) es una solución de infraestructura costo-efectiva para empresas pequeñas a grandes. Se utiliza para intercomunicar computadores y recursos mediante una transmisión remota, tal como se funciona con una red local. Estas redes utilizan en parte recursos de redes públicas como Internet.

Una VPN (Virtual Private Network) brinda a usuarios remotos los mismos accesos, sobre una red pública, como si ellos estuvieran en una red privada, permitiéndoles ahorrar dinero usando VPN sobre conexiones a Internet existentes, lo que implica una ventaja sobre redes privadas que usan líneas rentadas o Frame Relay.

Además los servicios de VPN incluyen autentificación, integridad de datos y encriptación. Por lo tanto una VPN es un túnel encriptado y seguro.

Actualmente las redes se han convertido en un factor crítico para cualquier organización. Cada vez en mayor medida, las redes transmiten información vital para el éxito de las empresas y dichas redes deben cumplir con atributos tales como seguridad, fiabilidad, alcance geográfico y efectividad en costos.

Lo dispositivos de redes como son los Switches y los Router brindan un gran apoyo a las redes privadas virtuales, por que están diseñados para trabajar en este tipo de tecnología. El propósito del Switch es concentrar la conectividad, haciendo que la transmisión de datos sea más eficiente. El Router esta diseñado para segmentar la red, con la idea de limitar tráfico de Broadcast y proporcionar seguridad, control y redundancia entre dominios individuales de Broadcast, también puede dar servicio de Firewall y un acceso económico a una WAN.

OBJETIVOS

- Sintetizar los conceptos de LANs virtuales (VLAN) como una alternativa para aprovechar al máximo el rendimiento de los Switches de capa 2 y capa 3, reduciendo los dominios de colisión y brindándole más seguridad y velocidad a una red LAN.

- Dar a conocer los diferentes tipos de VLAN con una descripción general de cada una de ellas en cuanto a sus ventajas y desventajas.

- Ilustrar algunos dispositivos que existen en el mercado que soportan VLAN, para comentar que soluciones están ofreciendo las diferentes compañías.

- Dar a conocer los conceptos básicos de VPN, para entender el funcionamiento de las ellas en las redes WAN.

- Describir conceptos sobre seguridad en redes como: cifrado, autenticación, integridad y no repudiación.

  Además, los diferentes protocolos de seguridad como: PPP, IPSec, PPTP y L2TP, para entender la importancia de la seguridad en las VPN y el porqué de los túneles.

- Mostrar en forma global y resumida una solución VPN para redes seguras y de bajo costo, utilizando una red pública como Internet en entornos WAN.

- Ilustrar y comentar algunos dispositivos que existen en el mercado que soportan VPN, para saber con que recursos se puede trabajar para implementar una red de este tipo.

- Implementar prácticas de V-LAN y VPN para afianzar los conceptos de redes privadas virtuales, con el fin de elaborar unas guías para los estudiantes, profesores y cualquier persona interesada en este tema.

1. REDES VIRTUALES A TRAVÉS DE ENLACES LAN (VLAN)

1.1 ANTECEDENTES DE VLAN

Los grupos de trabajo en una red común, se crean por la asociación física de los usuarios en un mismo segmento de red, o en un mismo concentrador o Hub, estos grupos de trabajo comparten el ancho de banda disponible y los dominios de "Broadcast" con la necesidad de la gestión del administrador de la red cuando se producen cambios en los miembros del grupo. Además es importante el hecho de la limitación geográfica que supone que los miembros de un determinado grupo de trabajo deben estar situados de forma continua, por su conexión al mismo segmento de la red o concentrador.

La técnica más utilizada para aumentar anchos de banda en las LANs es la conmutación (manejada mediante *Switches)*. Con los Switches se crean pequeños dominios, llamados segmentos, conectando un pequeño Hub de grupo de trabajo a un puerto de Switch o bien se aplica micro-segmentación la cual se realiza conectando cada estación de trabajo y cada servidor directamente a puertos del Switch teniendo una conexión dedicada dentro de la red, con lo que se consigue aumentar considerablemente el ancho de banda a disposición de cada usuario.

1.2 DEFINICIÓN DE VLAN

La tecnología de VLAN se basa en el empleo de Switches, en lugar de Hubs o concentradores, esto permite un control más inteligente del tráfico de la red, para que la eficiencia de la red entera se incremente. Por otro lado, al distribuir a los usuarios de un mismo grupo lógico a través de diferentes segmentos, se logra el incremento del ancho de banda en dicho grupo de usuarios.

Las LANs virtuales (VLANs) son agrupaciones de estaciones, definidas por software, que se comunican entre sí como si estuvieran conectadas al mismo concentrador, aunque se encuentren situadas en segmentos diferentes de una red de edificio o de campus. Es decir, la red virtual es la tecnología que permite separar la visión lógica de la red de su estructura física.

El Router que interconecta cada Hub compartido normalmente proporciona segmentación y puede actuar como Firewall de Broadcast. Los segmentos creados por los Switches no lo hacen. La segmentación tradicional de las LAN no agrupa a los usuarios según su asociación de grupo de trabajo o necesidad de ancho de banda. Por lo tanto, comparten el mismo segmento y ocupan el mismo ancho de banda, aunque los requisitos de ancho de banda varían enormemente por grupo de trabajo o departamento.

La siguiente figura muestra la diferencia entre segmentación tradicional y usando VLANs.

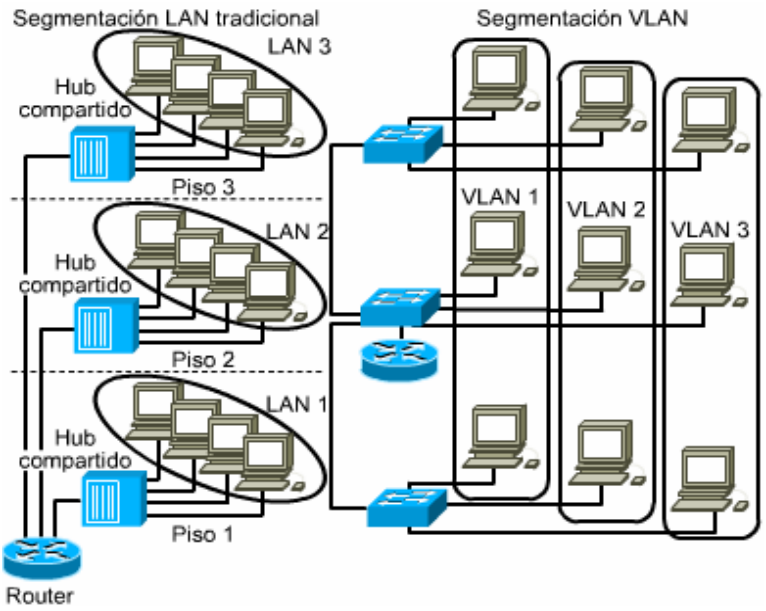


Figura 1.1 Diferencia entre segmentación tradicional y segmentación VLAN

1.3 VENTAJAS PARA IMPLEMENTAR VLAN

1.3.1 Control y conservación del ancho de banda

El tráfico de Broadcast se produce en todas las redes. La frecuencia de Broadcast depende de los tipos de aplicaciones, los tipos de servidores, la

cantidad de segmentación lógica y la manera en que se usan estos recursos de red.

La conmutación LAN compensa la escasez de ancho de banda y los cuellos de botella de la red, como los que aparecen entre varios PC y un servidor de archivos remoto. Esto crea dominios libres de colisión a partir de un dominio de colisión grande.

Una de las medidas más efectivas es segmentar de manera adecuada la red, con Firewalls de protección. Así, aunque un segmento puede presentar condiciones de Broadcast excesivas, el resto de la red se encuentra protegido con un Firewall, normalmente proporcionado por un Router.

Cuando no se colocan routers entre los Switches, los Broadcasts se envían a cada puerto del Switch. Esto normalmente se denomina red plana, donde hay un solo dominio de Broadcast para toda la red.

Las VLAN son un mecanismo efectivo para extender los Firewalls desde los routers a la estructura de los Switches y proteger la red contra problemas de Broadcast potencialmente peligrosos.

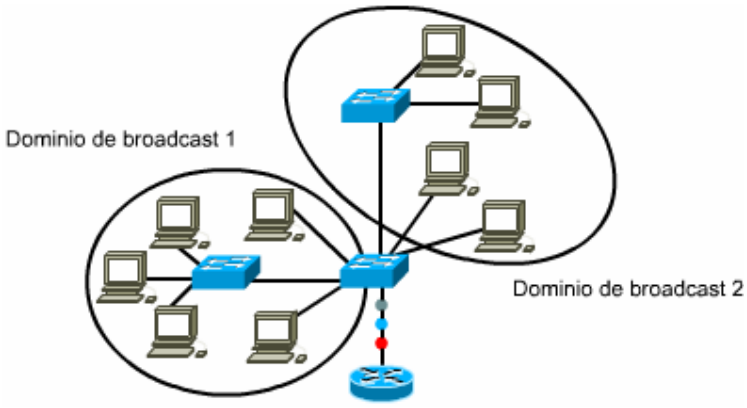


Figura 1.2 Dominio de Broadcast

El tráfico de Broadcast dentro de una VLAN no se transmite fuera de la VLAN. Por el contrario, los puertos adyacentes no reciben ningún tráfico de Broadcast generado desde otras VLAN. Este tipo de configuración reduce sustancialmente el tráfico total de Broadcast, libera el ancho de banda para el tráfico real de usuarios, y reduce la vulnerabilidad general de la red a las tormentas de Broadcast.

1.3.2 Seguridad

Los datos confidenciales requieren seguridad implementada a través de limitación del acceso. Uno de los problemas de las LAN compartidas es que son relativamente fáciles de penetrar. Un intruso puede conectarse a un puerto activo y tener acceso a todo el tráfico dentro de un segmento. Cuanto mayor sea el grupo, mayores serán las posibilidades de acceso.

Una técnica de administración económica y sencilla para aumentar la seguridad es segmentar la red en múltiples grupos de Broadcast que permitan que el administrador limite la cantidad de usuarios en un grupo de VLAN y evite que otro usuario se conecte sin recibir antes la aprobación.

En la VLAN segura, el Switch limita el acceso al grupo. Las restricciones se pueden implementar según la necesidad de seguridad de la empresa. En una VLAN segura, el Router limita el acceso a la VLAN según la configuración del Switch y del Router. Se pueden colocar restricciones sobre direcciones de estación, tipos de aplicación, tipos de protocolo e inclusive según la hora.

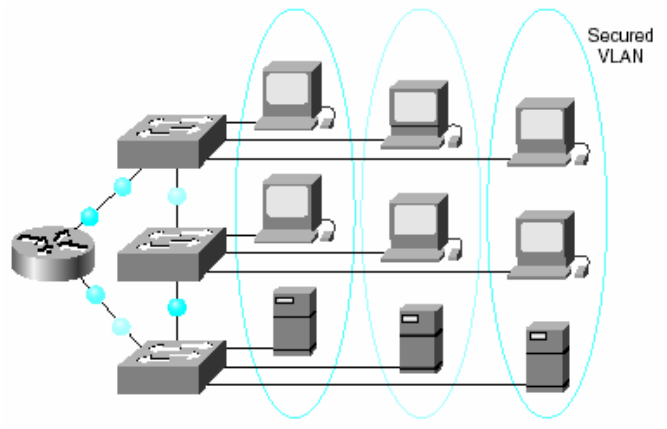


Figura 1.3 Seguridad en V-LAN

1.3.3 Protección de la inversión

La capacidad de una VLAN está incluida en el precio de los Switches que las ofrecen, y su uso no requiere cambios en la estructura de la red o cableado,

sino más bien los evitan, facilitando las reconfiguraciones de la red sin costos adicionales. Además, los administradores de redes ahorran dinero conectando los Hubs existentes a los Switches.

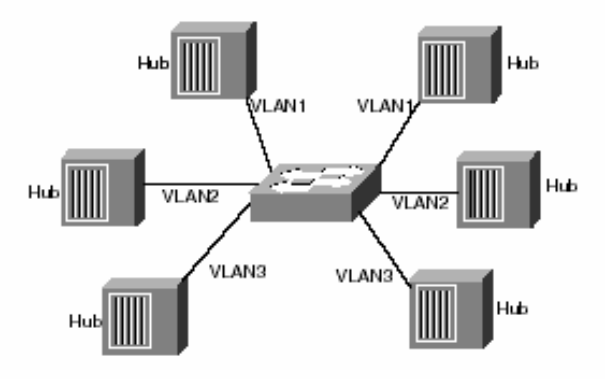


Figura 1.4 VLAN usando HUB

Cada segmento de Hub conectado a un puerto de Switch se puede asignar a sólo una VLAN. Las estaciones que comparten un segmento de Hub se asignan todas al mismo grupo de VLAN. Cuanto más el Hub compartido se pueda subdividir en grupos más pequeños, mayor será la microsegmentación y la flexibilidad de la VLAN para asignar usuarios individuales a los grupos de VLAN.

1.3.4 Otras ventajas para implementar V-LAN

Otras Razones fundamentales para implementar VLAN son:

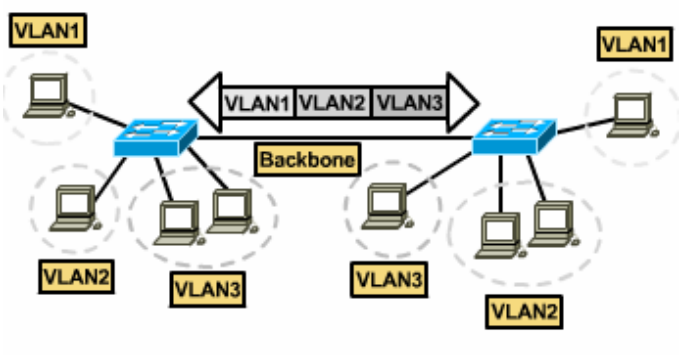


Figura 1.5 Las VLAN separan dominios lógicos

1. Movilidad: el punto fundamental de las redes virtuales es el permitir la movilidad física de los usuarios dentro de los grupos de trabajo.

2. Dominios lógicos: los grupos de trabajo son independientes de sus conexiones físicas, ya que están constituidos como dominios lógicos.

3. Conectividad: los modelos con funciones de Routing nos permiten interconectar diferentes Switches y expandir las VLAN a través de ellos, incluso aunque estén situados en lugares geográficos diversos.

1.4 CARACTERÍSTICAS DE UNA VLAN

- El núcleo de una VLAN es un Switch.

- Una VLAN es una red Switchada que está lógicamente segmentada en base a funciones, grupos de proyectos o usuarios compartiendo la misma aplicación, sin importar la ubicación física de los usuarios.

Por ejemplo, cada puerto del Switch puede asignarse a una VLAN. Los puertos que no pertenecen a esa VLAN no comparten los Broadcast. Esto mejora el comportamiento global de la red.

- Agrupando puertos y usuarios a través de múltiples Switches, la VLAN puede cubrir un edificio completo, interconectar edificios, o aun redes WAN.

- Las VLANs deben ser rápidas basadas en Switches, porque los routers no dan la velocidad requerida, su información deberá viajar a través del Backbone y deberán ser movibles, es decir, que el usuario no tenga que reconfigurar la maquina cada vez que se cambie de lugar.

- Mediante las VLANs podemos crear un nuevo grupo de trabajo, con tan solo una reconfiguración del software del conmutador. Ello evita el recableado de la red o el cambio en direcciones de subredes, permitiéndonos así asignar el ancho de banda requerido por el nuevo grupo de trabajo sin afectar a las aplicaciones de red existentes.

1.5 TIPOS DE VLAN

Existen cuatro tipos principales de VLAN:

- VLAN basadas en puertos, estática o implícitas.
- VLAN basadas en puerto central.
- VLAN basadas en dirección MAC o explicitas.
- VLAN basadas en filtros, reglas o protocolos.

1.5.1 V-LAN por puerto o implícitas

Este tipo de VLAN es la más sencilla, cada puerto del Switch puede asociarse a una VLAN. No necesitan cambios en la trama, pues de la misma forma que reciben información la procesan.

La figura 1.6, nos muestra el esquema de la configuración basada en puerto:

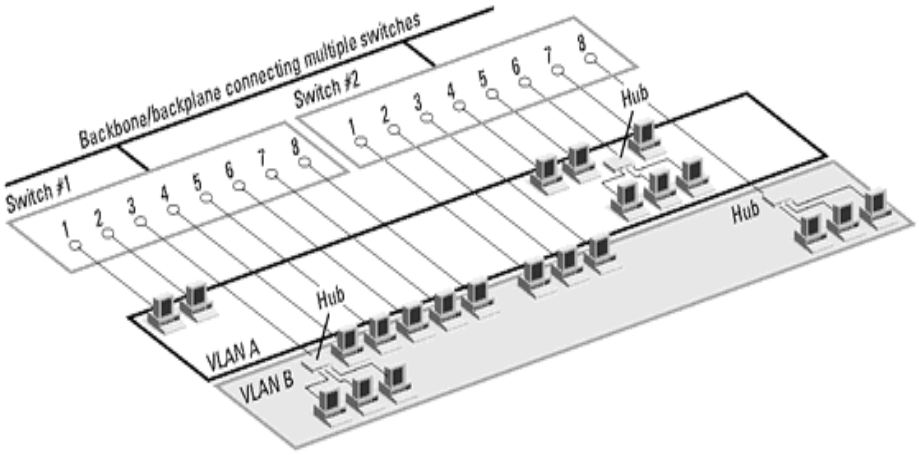


Figura 1.6 VLAN por puerto

Ventajas:

- Facilidad de movimientos y cambios: Un movimiento supone que la estación cambia de ubicación física, pero sigue perteneciendo a la misma VLAN.

  Requiere re-configuración del puerto al que se conecta la estación, salvo si se utilizan técnicas de asignación dinámica a VLAN, aunque existen algunas aplicaciones gráficas de gestión de VLANs que automatizan totalmente está reasignación.

- Micro-segmentación y reducción del dominio de Broadcast: Aunque los Switches permiten dividir la red en pequeños segmentos, el tráfico Broadcast sigue afectando el rendimiento de las estaciones y se requieren enrutadores o VLANs para aislar los dominios de Broadcast. La definición de VLAN por puerto implica que el tráfico

Broadcast de una VLAN no afecta a las estaciones en el resto de las VLANs, puesto que es siempre interno a la VLAN en la que se origina.

1.5.2 V-LAN por puerto central

En las VLAN de puerto central, a todos los nodos conectados a puertos en la misma VLAN se les asigna el mismo identificador de VLAN. El gráfico muestra la pertenencia a la VLAN por puerto, lo que facilita el trabajo del administrador y hace que la red sea más eficiente porque:

- Los usuarios se asignan por puerto.
- Las VLAN son de fácil administración.
- Proporciona mayor seguridad entre las VLAN.
- Los paquetes no se "filtran" a otros dominios.

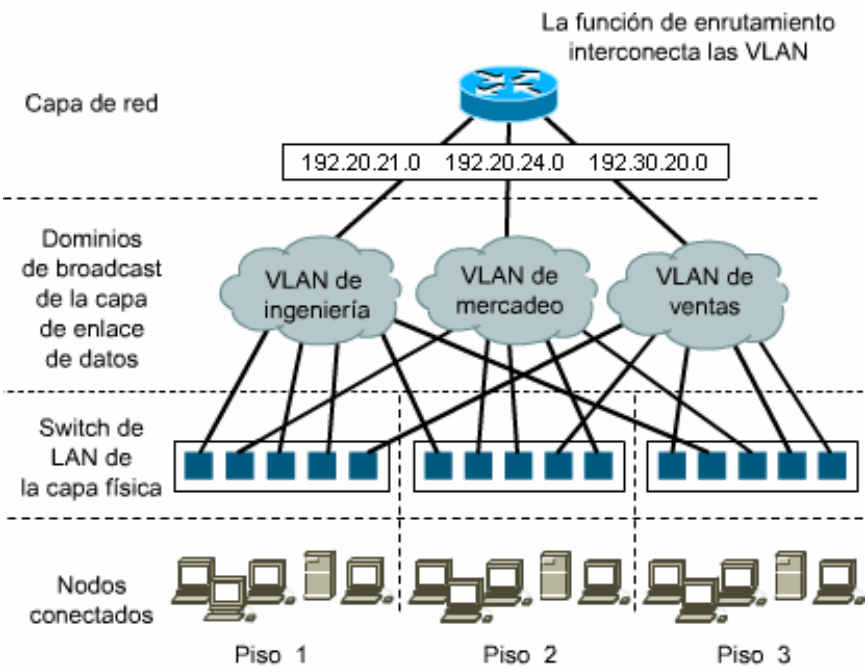


Figura 1.7 VLAN por puerto central

1.5.3 V-LAN por dirección MAC

La relación de pertenencia a la VLAN se basa en la dirección MAC.

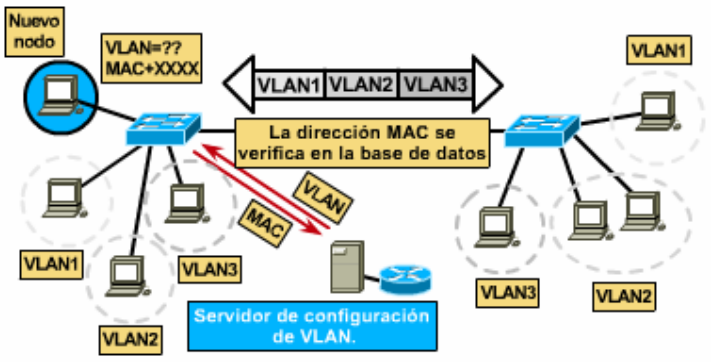


Figura 1.8 VLAN por dirección MAC

Ventajas:

- Facilidad de movimientos: Las estaciones pueden moverse a cualquier ubicación física perteneciendo siempre a la misma VLAN sin que se necesite ninguna re-configuración del Switch.

- Multiprotocolo: No presenta ningún problema de compatibilidad con los diversos protocolos y soporta incluso la utilización de protocolos dinámicos tipo DHCP.

Desventajas:

- Problemas de rendimiento y control de Broadcast: Este método de definición de VLAN implica que en cada puerto del Switch coexisten miembros de distintas VLANs por lo que cualquier tráfico Broadcast afecta al rendimiento de todas las estaciones.

- Complejidad en la administración: Todos los usuarios deben configurarse inicialmente en una VLAN. El administrador de la red introduce de forma manual, en la mayoría de los casos, todas las direcciones MAC de la red que se encuentran en algún tipo de base de datos. Cualquier cambio o nuevo usuario requiere modificación de la base de datos. Todo ello puede complicarse extremadamente con redes con un gran número de usuarios o Switches.

  Existen soluciones alternativas para automatizar esta definición y normalmente se utiliza un servidor de configuración de forma que las

direcciones MAC se copian de las tablas de direcciones de los Switches a la base de datos del servidor. La asignación dinámica de VLAN basándose en direcciones MAC es también posible, aunque su implementación puede ser muy compleja.

Una V-LAN por MAC puedo ser desarrollada, utilizando Switch Catalyst 5000 o Switch Catalyst 6000 series de Cisco, porque IOS de estos Switch soportan el programa VMPS. Los Switch de Cisco con serires inferiores a 5000, no soportan este tipo de V-LAN.

VMPS *(V-LAN Memberchip Policy Server) s*ervicio de seguridad para usuarios de V-LAN: VMPS asigna direcciones MAC a cada VLAN.
VMPS contiene una base de datos que el administrador crea, donde se encuentra todas las direcciones MAC y las V-LAN a la que pertenecen.
Los archivos de la base de dato contiene la información VMPS: nombre de dominio, nombre de V-LAN y dirección MAC para la V-LAN.

VMPS verifica si la MAC del usuario que quiere acceder a la V-LAN haga parte de la tabla de MAC del servidor. Si la MAC no es aprobada, VMPS envía una respuesta de negación al cliente, sino VMPS permite al usuario acceder a la V-LAN

1.5.4 V-LAN por filtro o protocolo

La asignación a las VLANs se basa en información de protocolos de red (por ejemplo: dirección IP o dirección IPX y tipo de encapsulamiento). La pertenencia a la VLAN se basa en la utilización de unos filtros que se aplican a las tramas para determinar su relación de pertenencia a la VLAN. Los filtros han de aplicarse por cada trama que entre por uno de los puertos del Switch.

Ventajas:

- Segmentación por protocolo: es el método apropiado sólo en aquellas redes en las que el criterio de agrupación de usuarios esté basado en tipo de protocolo de nivel 3.
- Asignación dinámica: tanto la definición de VLANs por dirección MAC como por protocolo de nivel 3, ayudan a automatizar la configuración del puerto del Switch.

Desventajas:

- Problemas de rendimiento y control de Broadcast: La utilización de las VLANs de nivel 3 requiere complejas búsquedas en tablas de

pertenencia que afectan al rendimiento global de Switch. Los retardos de transmisión pueden aumentar entre un 50% y un 80%.

El problema de control de Broadcast surge con las estaciones Multiprotocolo o sistema de multistack (por ejemplo estaciones con stacks TCP/IP, IPX y AppleTalk) que pertenecen a tantas VLANs como protocolos utilizan y por lo tanto recibirán todos los Broadcast provenientes de las diversas VLANs en las que están incluidas.

- No soporta protocolos de nivel 2 ni protocolos dinámicos: La estación necesita una dirección de nivel 3 para que el Switch la asigne a una VLAN. Si existen protocolos dinámicos como DHCP y la estación no tiene configurada su dirección IP ni su enrutador por defecto, el Switch no puede clasificar la estación dentro de una VLAN.

1.5.5 Otros tipos de V-LAN

Además de las VLAN mencionadas, existen otros tipos de VLAN:

- VLAN por subredes de IP o IPX

Aparte de la división que ejecuta la VLAN por protocolo, existe otra subdivisión dentro de esta para que el usuario, aunque este conectado a la VLAN del protocolo IP, sea asignado en otra VLAN (subred).

- VLAN Binding

Se conjugan tres parámetros o criterios para la asignación de VLAN: si el usuario es del puerto x, entonces se le asignara una VLAN correspondiente. También puede ser puerto, protocolo y dirección MAC, pero lo importante es cubrir los tres requisitos previamente establecidos, ya que cuando se cumplen estas tres condiciones se coloca al usuario en la VLAN asignada, pero si alguno de ellos no coincide, entonces se rechaza la entrada o se manda a otra VLAN.

- VLAN por DHCP

No es necesario proporcionar una dirección IP, sino que cuando el usuario enciende la computadora automáticamente el DHCP pregunta al servidor para que tome la dirección IP y con base en esta acción asignar al usuario a la VLAN correspondiente.

- VLAN definidas por el usuario

En esta política de VLAN puede generar un patrón de bits, para cuando llegue el frame. Ejemplo: si los primeros cuatro bits son 1010 se irán a la VLAN de ingeniería, sin importar las características del usuario, protocolo, dirección MAC o puerto. Si el usuario manifiesta otro patrón de bits,

entonces se trasladara a la VLAN que le corresponda; aquí el usuario define las VLAN.

1.6 EJEMPLOS DE DISPOSITIVOS QUE SOPORTAN VLAN

El primer suministrador de conmutadores con soporte VLAN fue ALANTEC (familia de concentradores/conmutadores multimedia inteligentes PowerHub), pero actualmente son muchos los fabricantes que ofrecen equipos con soluciones VLAN: Bytex (concentrador inteligente 7700), Cabletron (ESX-MIM), Chipcom (*OnLine*), Lannet (MultiNet Hub), Synoptics (Lattis System 5000), UB (Hub *Access/One*), 3Com (LinkBuilder) y Cisco.

Los modelos más avanzados de conmutadores con funciones VLAN, soportan filtros muy sofisticados, definidos por el usuario o administrador de la red, que permiten determinar con gran precisión las características del tráfico y de la seguridad que se desea en cada dominio, segmento, red o conjunto de redes.

En la actualidad, las implementaciones de tecnologías de redes virtuales no son ínter-operativos entre diferentes productos de diversos fabricantes. Muchos de los fabricantes intentan buscar soluciones adecuadas para lograr interoperatividad, y por ello, una gran ventaja de las soluciones basadas en software es que podrán ser adaptadas a las normalizaciones que tendrán lugar en un futuro cercano. Algunas soluciones basadas en hardware habrán de quedarse atrás en este sentido.

◊ TE100-S1616V

Conmutador VLAN de 16 puertos y 10/100mbps

Figura 1.9 Switch TE100-S1616V

- Características
  - Conforme con las normas IEEE 802.3 para Ethernet de 10/100Mbps y IEEE 802.3u
  - 16 puertos con auto detección 10/100Mbps
  - Soporte para cuatro redes virtuales (VLANs) basadas en puertos
  - Funcionamiento en todos los puertos UTP y fibra óptica
  - Aprendizaje automático de la configuración de red
  - Indicadores LEDs de alta visibilidad

◊ Tarjetas de red EtherLink III 10/100 NIC para clientes y tarjetas de red 10/100 Gigabit Ethernet NIC para servidor con software Dynamic*Access (3COM)*

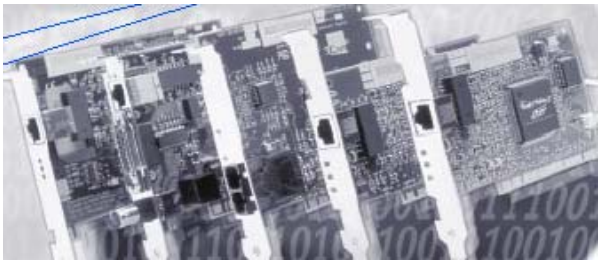


Figura 1.10 Tarjetas de red EtherLink III 10/100

- Características

Las tarjetas de red y los conmutadores 3Com le permiten configurar redes de área local virtuales (VLAN), estas redes virtuales constituyen un método sencillo para mantener el tráfico de red de los departamentos o de los grupos de trabajo, de modo que no se vea afectado el rendimiento de toda la LAN y exista un mayor nivel de seguridad para los datos.

2. REDES PRIVADAS VIRTUALES (VPN)

2.1. ANTECEDENTES DE REDES PRIVADAS VIRTUALES

Una de las necesidades vitales de las organizaciones modernas es la posibilidad de compartir información con sedes en diferentes zonas y secciones de la organización que no se encuentran en el mismo entorno físico.

Las compañías tienen la posibilidad de crear una red privada virtual que demanda una inversión relativamente pequeña de hardware para la conexión entre los puntos de la red. Durante un tiempo, las grandes corporaciones habían solucionado el problema mediante sistemas de comunicación como líneas punto a punto y sofisticadas instalaciones de interconexión. Aunque efectivas, estas soluciones quedaban fuera del alcance de organizaciones de menor tamaño y con recursos económicos y técnicos más escasos.

Las últimas alternativas de comunicación, han hecho que la desventaja operativa desaparezca, permitiendo que pequeñas y medianas empresas dispongan de su propia red de comunicación privada, para intercomunicarse y compartir información de forma sencilla y segura, con inversiones muy inferiores a las de hace muy poco tiempo.

Las LAN tradicionales son redes esencialmente restringidas, por lo cual se puede intercambiar información entre las computadoras sin pensar en la seguridad de la información.

2.2 DEFINICIÓN DE RED PRIVADA VIRTUAL

Una Red Privada Virtual (VPN) es una forma de compartir y transmitir información entre un círculo cerrado de usuarios que están situados en diferentes localizaciones, mediante un proceso de comunicación cifrado o encapsulado que trasfiere datos desde un punto hacia otro de manera segura, y los datos que se transfieren pasan a través de una red abierta, insegura y enrutada.

Las redes privadas virtuales crean un túnel o conducto dedicado de un sitio a otro y son una alternativa de bajo costo, para usar líneas alquiladas que conecten sucursales o para hacer negocios. Los datos se encriptan protegiendo la información, por medio de un proceso de encapsulación de los paquetes de datos a distintos puntos remotos mediante el uso de infraestructuras públicas o privadas de transporte, para reducir las responsabilidades de gestión de una red local.

Las VPN usan protocolos especiales que permiten encriptar información y permiten únicamente a la persona autorizada desencriptar esa información

con un identificador que comprueba que la transmisión se ha hecho desde una fuente confiable.

Las VPN también pueden utilizarse en líneas rentadas, enlaces ATM/Frame Relay (retransmisión de tramas) o servicio de Red telefónica simple (POTN), como las redes digitales de servicios integrados (ISDN) y las Líneas de suscripción digital (xDSL).

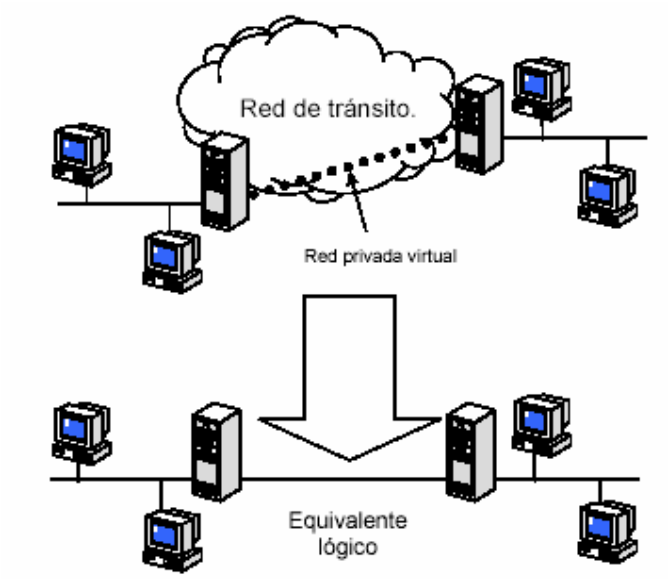


Figura 2.1 Red Privada Virtual

2.3 RAZONES PARA IMPLEMENTAR Y NO IMPLEMENTAR UNA VPN

Algunas de las razones por la que muchas empresas utilizan las VPN son las siguientes:

• Algunas VPN utilizan Internet como su medio de transporte, lo cual reduce los costos, en cuanto a instalación, mantenimiento y administración de una red.

• Necesidad de un alcance global de bajo costo, porque Internet es un medio propicio tanto para clientes comerciales como privados, que se extiende por todo el mundo.

• Las VPNs son flexibles, porque la arquitectura de las VPN es independiente del medio de acceso o mecanismo de comunicación pudiéndose optar por múltiples tecnologías o proveedores de servicio. Esto permite que la red de comunicación se adapte a los requerimientos de los negocios.

• Las VPNs son escalables geográficamente porque el desarrollo masivo de redes, permite que la empresa tenga puntos de presencia de su red en lugares donde antes era imposible. Por otro lado la independencia respecto a la tecnología de acceso permite la escalabilidad del ancho de banda de la red de acuerdo a los requerimientos del negocio de la empresa. Incluso la escalabilidad de la red comúnmente, no incide en la administración y gestión de esta.

• La tecnología base de las VPN es el conjunto de protocolos TCP/IP, lo cual la hace más fácil de comprender e implementar que una tecnología completamente nueva.

Las razones más importantes para no implementar VPN son:

• Donde el desempeño es crítico (si se usa la red pública de Internet y no líneas dedicadas).

• Donde los protocolos sin normas no pueden encapsularse con el protocolo IP (si se usa la red pública de Internet), en el caso de líneas dedicadas se pueden implementar otro protocolo.

2.4 REQUERIMIENTOS Y COMPONENTES BÁSICOS DE SEGURIDAD DE UNA VPN

Si una compañía desea facilitar un acceso controlado a los recursos y a la información de la compañía, la solución deberá permitir la libertad para que los clientes autorizados se conecten fácilmente a los recursos corporativos de la red de área local (LAN), y la solución también deberá permitir que las oficinas remotas se conecten entre sí para compartir recursos e información (conexiones de LAN a LAN). Finalmente, la solución debe garantizar la privacidad y la integridad de los datos al viajar a través de Internet público.

Por lo tanto, como mínimo, una solución de VPN debe proporcionar todo lo siguiente:

• Autenticación de usuario

La solución deberá verificar la identidad de un usuario y restringir el acceso a la VPN a usuarios no autorizados. Además, la solución deberá proporcionar registros de auditoria y contables para mostrar quién accedió a qué información y cuándo.

Cuándo se evalúan soluciones VPNs, es importante considerar una solución que tenga los mecanismos de autenticación de datos (firma digital o integridad de los datos) y autenticación de usuarios (verificación de la identidad del usuario).

• Administración de dirección

La solución deberá asignar una dirección al cliente en la red privada y deberá asegurarse que las direcciones privadas se mantengan así.

• Administración de llaves

La solución deberá generar y renovar las llaves de encriptación para el cliente y para el servidor.

• Encriptación de datos

Los datos que viajan en una red pública no podrán ser leídos por clientes no autorizados. Las técnicas de encripción son usadas para convertir un texto claro en un texto cifrado. Una vez que el mensaje es convertido en un texto

cifrado, es enviado, luego quien lo reciba se encargara de desencriptar el texto cifrado convirtiéndolo en el texto claro otra vez.

• Soporte de protocolo múltiple

La solución deberá poder manejar protocolos comunes utilizados en las redes públicas. Estos incluyen protocolo de Internet (IP), central de paquete de Internet (IPX), etc.

• Certificados

Con la encriptación, tanto el remitente como el destinatario cuentan con una llave secreta compartida. El remitente utiliza una llave privada para encriptar o firmar digitalmente los mensajes, mientras que el receptor utiliza una llave pública para descifrar estos mensajes. La llave pública puede distribuirse libremente a todos los que necesiten recibir mensajes encriptados o firmados digitalmente. El remitente necesita proteger cuidadosamente sólo la llave privada.

Para garantizar la integridad de la llave pública se publica con un certificado.

IPSec puede utilizar de manera opcional este método para la autenticación de extremo a extremo.

2.5 ÁREAS DONDE SE PUEDE IMPLEMENTAR UNA VPN

Las VPN se aplican en las siguientes áreas:

2.5.1 VPN de Intranet

Una VPN de Intranet se crea entre una oficina central corporativa y varias oficinas remotas, o entre las oficinas centrales y las oficinas dependientes, a través de una red pública, mediante enlace dedicado al Proveedor de Servicio. La VPN goza de las mismas cualidades que la red privada: seguridad, calidad de servicio, disponibilidad, etc.

Figura 2.2 VPN de Intranet

Normalmente, sólo se utiliza dentro de la red de una compañía y únicamente acceden los empleados de la misma, pero el acceso viene desde el exterior y no del interior.

2.5.2 VPN de acceso remoto (VPDN)

Una VPN de acceso remoto se crea entre oficinas centrales y usuarios móviles remotos. Con el software de cifrado en un PC, un individuo establece un túnel cifrado al dispositivo de la VPN en oficinas centrales.

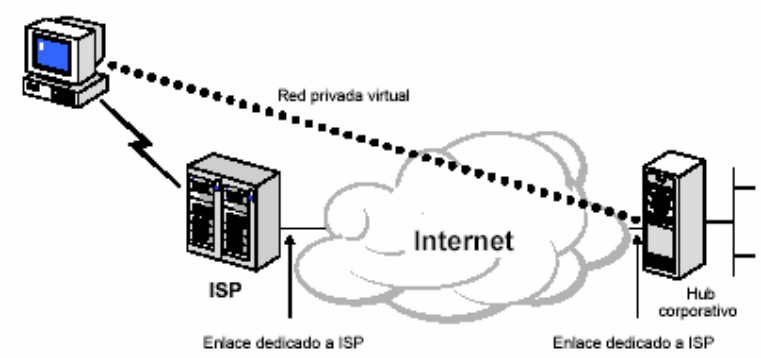


Figura 2.3 Uso de una VPN para conectar a un cliente remoto con una LAN privada

Uno de los protocolos que utiliza las VPN de acceso remoto es L2TP.

La VPN de acceso remoto permite el uso de múltiples tecnologías como discado, ISDN, xDSL, cable, o simplemente IP para la conexión segura de usuarios móviles o sucursales remotas a los recursos corporativos.

2.5.3 VPN de Extranet

Una VPN de Extranet se crea entre la empresa y sus clientes o proveedores. La Extranet permitirá el acceso con el protocolo PPP normal utilizado por los navegadores Web actuales, o permitirá que se realice la conexión utilizando otros servicios y protocolos acordados por las partes involucradas.

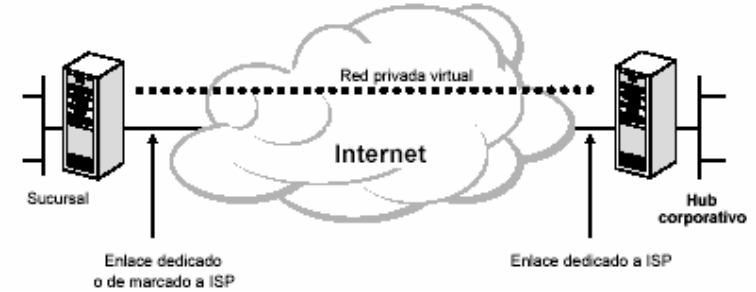


Figura 2.4 VPN de Extranet

Esta configuración le dará a la empresa la capacidad para realizar transacciones de manera segura y efectiva con sus clientes y socios.

2.6 ASPECTOS BÁSICOS DE TÚNELES EN UNA VPN

Trabajar en un sistema de túnel es un método que utiliza una infraestructura de la red para transferir datos de una red sobre otra. Los datos que serán transferidos (o carga útil) pueden ser las tramas (o paquetes) de otro protocolo. En lugar de enviar una trama a medida que es producida por el nodo, el protocolo de túnel encapsula la trama en un

encabezado adicional. El encabezado adicional proporciona información de enrutamiento.

La trayectoria lógica a través de la cual viajan los paquetes encapsulados en la red se le llama un túnel. Una vez que las tramas encapsuladas llegan a su destino sobre la red se desencapsulan y se envían a su destino final.

Una solución de VPN basada en un Protocolo de túnel punto a punto, cumple con todos requerimientos básicos y aprovecha la amplia disponibilidad de Internet. Otras soluciones, incluyendo el Protocolo de seguridad IP (IPSec), cumplen con algunos de estos requerimientos, y siguen siendo útiles para situaciones específicas.

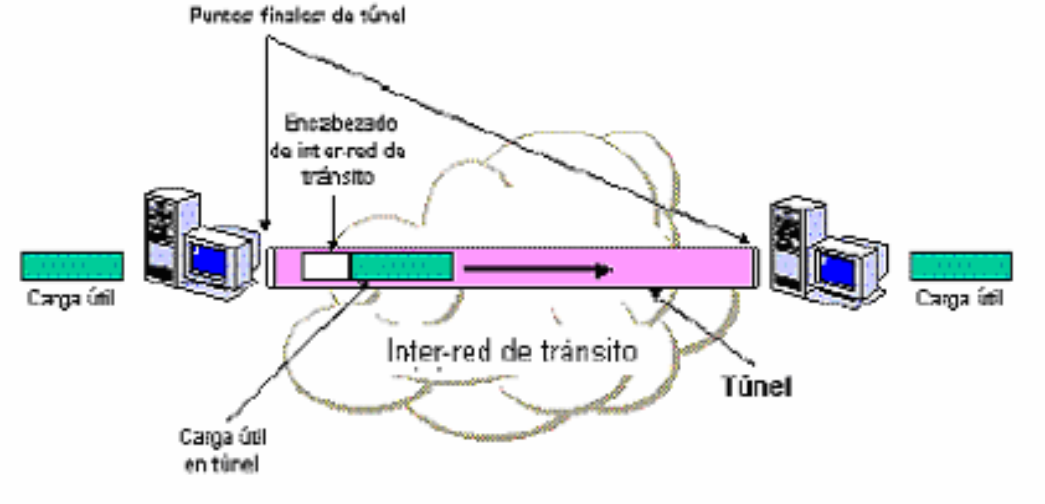


Figura 2.5 Túneles

Las tecnologías de túnel existen desde hace tiempo. Algunos ejemplos de tecnologías incluyen:

• Túneles IPX para Novell NetWare: cuando un paquete IPX se envía a un servidor NetWare o ruteador IPX, el servidor o ruteador envuelve el paquete IPX en un encabezado UDP e IP, y luego lo envía a través de una Interred IP.

• Protocolo de túnel de punto a punto (PPTP): PPTP permite que se encripte el tráfico IP, IPX o NetBEUI y luego se encapsule en un encabezado IP para enviarse a través de una red corporativa IP o una red pública IP, como Internet.

• Protocolo de túnel de nivel 2 (L2TP): L2TP permite que se encripte el tráfico IP, IPX o NetBEUI y luego se envíe sobre cualquier medio que dé soporte a la entrega de datagramas punto a punto, como IP, X.25, *Frame Relay* o AT*M.*

• Modo de túnel de seguridad IP (IPSec): El modo de túnel IPSec permite que se encripten las cargas útiles IP y luego se encapsulen en un encabezado IP para enviarse a través de una red corporativa IP o una red pública IP como Internet.

2.7 CÓMO FUNCIONAN LOS TÚNELES EN UNA VPN

Para las tecnologías de túnel de Nivel 2 como PPTP y L2TP, un túnel es similar a una sesión; los dos puntos finales del túnel deben estar de acuerdo respecto al túnel y deben negociar las variables de la configuración, como son asignación de dirección o los parámetros de encriptación o de compresión.

Por lo general, las tecnologías del túnel de Nivel 3 suponen que se han manejado manualmente todos los temas relacionados con la configuración. Para los protocolos de Nivel 2 (PPTP y L2TP), se debe crear, mantener y luego dar por terminado un túnel.

Una vez que se establece el túnel, se pueden enviar los datos a través del mismo. El cliente o el servidor del túnel utilizan un protocolo de transferencia. Por ejemplo, cuando el cliente del túnel envía una carga útil al servidor del túnel, el cliente del túnel adjunta primero un encabezado de protocolo de transferencia de datos de túnel a la carga útil. Luego, el cliente envía la carga útil encapsulada resultante a través de la red, la cual lo enruta al servidor del túnel. El servidor del túnel acepta los paquetes, quita el encabezado del protocolo de transferencia de datos del túnel y envía la carga útil a la red objetivo.

2.8 PROTOCOLOS DE TÚNELES EN VPN

Para que se establezca un túnel tanto el cliente del túnel como el servidor del túnel deberán utilizar el mismo protocolo de túnel.

La tecnología de túnel se puede basar ya sea en el protocolo del túnel de Nivel 2 ó de Nivel 3. Los protocolos de nivel 2 corresponden al nivel de Enlace de datos, y utilizan tramas como su unidad de intercambio. PPTP, L2TP y L2F son protocolos de túnel de Nivel 2, estos encapsulan la carga útil en una trama de Protocolo de punto a punto (PPP).

Los protocolos de Nivel 3 corresponden al nivel de la red y utilizan paquetes, IP sobre IP y el modo de túnel de seguridad IP (IPSec) son ejemplos de los protocolos de túnel de Nivel 3. Estos protocolos encapsulan los paquetes IP en un encabezado adicional IP antes de enviarlos a través de una red IP.

2.8.1 Protocolo de punto a punto (PPP)

PPP se diseñó para enviar datos a través de conexiones punto a punto dedicadas y encapsula paquetes de IP, IPX y NetBEUI.

PPP aborda el problema de la conectividad con Internet empleando tres componentes:

- HDLC es protocolo que es utilizado por PPP para encapsular datagramas sobre enlaces series.
- Protocolo de control de enlace (LCP) es utilizado para establecer, configurar y probar la conexión de enlaces de datos.
- La familia de protocolos de control de red (NCP) es utilizada para establecer y configurar los distintos protocolos de capa de red.

Existen cuatro fases distintivas de negociación en una sesión de marcación PPP. Cada una de estas cuatro fases debe completarse de manera exitosa antes de que la conexión PPP esté lista para transferir los datos del usuario.

Fase1: Establecer el enlace del PPP

PPP utiliza el Protocolo de control de enlace (LCP) para establecer, mantener y terminar la conexión física. Durante la fase LCP inicial, se seleccionan las opciones básicas de comunicación. Durante la fase de establecimiento de enlace (Fase 1), se seleccionan los protocolos de Autenticación, pero no se implementan efectivamente hasta la fase de Autenticación de conexión (Fase 2).

Fase 2: Autenticar al usuario

En la segunda fase, la PC cliente presenta las credenciales del usuario al servidor de acceso remoto. Un esquema seguro de Autenticación proporciona protección contra ataques de reproducción y personificación de

clientes remotos. (Un ataque de reproducción ocurre cuando un tercero monitorea una conexión exitosa y utiliza paquetes capturados para reproducir la respuesta del cliente remoto, de tal manera que pueda lograr una conexión autenticada. La personificación del cliente remoto ocurre cuando un tercero se apropia de una conexión autenticada. El intruso espera hasta que se haya autenticado la conexión y luego atrapa los parámetros de conversación, desconecta al usuario autenticado y toma control de la conexión autenticada.)

Fase 3: Invocar los protocolo(s) a nivel de red

Una vez que se hayan terminado las fases previas, PPP invoca los distintos protocolos de control de red (NCPs) que se seleccionaron durante la fase de establecimiento de enlace (Fase1) para configurar los protocolos que utiliza el cliente remoto.

Fase4: Fase de transferencia de datos

Una vez que se han terminado las tres fases de negociación, PPP empieza a transferir datos. Cada paquete de datos transmitidos se envuelve en un encabezado del PPP el cual quita el sistema receptor. Si se seleccionó la compresión de datos en la fase 1 y se negoció en la fase 3, los datos se comprimirán antes de la transmisión. Si se seleccionaron y se negociaron de manera similar la encriptación de datos, los datos (comprimidos opcionalmente) se encriptarán antes de la transmisión.

La mayoría de las implementaciones del PPP proporcionan métodos limitados de Autenticación, típicamente el Protocolo de autenticación de contraseña (PAP), el Protocolo de autenticación de saludo Challenge (CHAP) y Microsoft Challenge Handshake Authentication Protocol (MSCHAP).

• Protocolo de autenticación de contraseña (PAP): PAP proporciona un método sencillo en que un nodo remoto establezca su identidad, utilizando un establecimiento de comunicación de dos vías. Una vez completada la fase de establecimiento del enlace PPP, el nodo remoto envía repetidas veces un par de nombres de usuario/contraseña por el enlace hasta que se obtiene el acuse de recibo de la autenticación o hasta que se cierra la conexión.

PAP no es un protocolo de autenticación sólido. Las contraseñas se envían a través del enlace en texto no cifrado, y no hay protección contra la reproducción o los ataques de ensayo y error. El nodo remoto tiene control de la frecuencia y la temporización de los intentos de conexión

• Protocolo de autenticación de saludo Challenge (CHAP): CHAP se utiliza para verificar periódicamente la identidad del nodo remoto, utilizando un saludo de tres vías. Esto se realiza durante el establecimiento inicial del enlace y se puede repetir en cualquier momento una vez que se ha establecido el enlace. CHAP ofrece funciones tales como verificación periódica para mejorar la seguridad. Esto hace que CHAP sea más efectivo que PAP. PAP realiza la verificación sólo una vez, lo que lo hace vulnerable

a los "Hackers" y a la reproducción por módem. Además, PAP permite que la persona que realiza la llamada intente realizar la autenticación a voluntad, lo que lo hace vulnerable a los ataques, mientras que CHAP no permite que la persona que realiza la llamada intente realizar la autenticación sin recibir un pedido de verificación.

Una vez que se ha completado la fase de establecimiento de enlace PPP, el host envía un mensaje de comprobación al nodo remoto. El nodo remoto responde con un valor. El host compara el valor de la respuesta con su propio valor. Si los valores concuerdan, se produce un acuse de recibo de la autenticación. De otro modo, la conexión se termina.

CHAP suministra protección contra los intentos de reproducción a través del uso de un valor de comprobación variable que es exclusivo e impredecible. El uso de comprobaciones reiteradas tiene como fin limitar el tiempo de exposición ante cualquier ataque único. El Router local (o un servidor de autenticación de terceros) tiene el control de la frecuencia y la temporización de las señales.

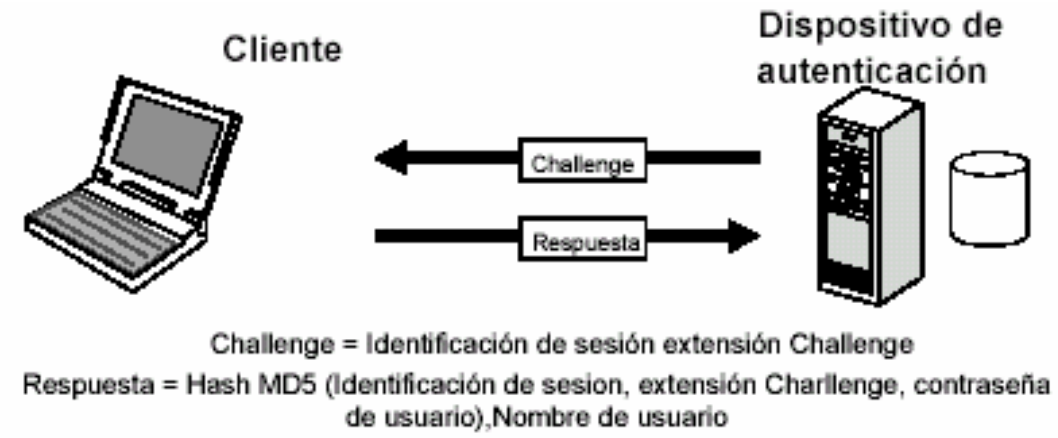


Figura 2.6 Autenticación CHAP

CHAP es un mecanismo de autenticación encriptado que evita la transmisión de contraseñas reales en la conexión. El cliente remoto deberá utilizar el algoritmo de control unidireccional MD5 para devolver el nombre del usuario y una encriptación del *challenge*, la identificación de la sesión y la contraseña del cliente.

- **Microsoft Challenge-Handshake Authentication Protocol (MS-CHAP):**

El MS-CHAP es un mecanismo de autenticación encriptado muy similar al CHAP. Envía un *challenge*, el cual consiste en una identificación de sesión. El cliente remoto debe devolver el nombre del usuario y una verificación MD4 de la extensión challenge, el identificador de sesión y la contraseña MD4 verificada. Esto, proporciona un nivel adicional de seguridad debido a que permite que el servidor almacene las contraseñas verificadas en lugar de contraseñas con texto transparente.

2.8.2 Protocolo de túnel de punto a punto (PPTP)

El PPTP es un protocolo de Nivel 2 que encapsula las tramas del PPP en datagramas. También se puede utilizar el PPTP en una red privada de LAN a LAN. El protocolo de túnel de punto a punto (PPTP) utiliza una conexión TCP para mantenimiento del túnel y tramas del PPP encapsuladas para datos de túnel. Se pueden encriptar y/o comprimir las cargas útiles de las tramas del PPP.

2.8.3 Reenvío de nivel 2 (L2F)

L2F, una tecnología propuesta por Cisco, es un protocolo de transmisión que permite que los servidores de acceso de marcación incluyan el tráfico de marcación en el PPP y lo transmitan sobre enlaces WAN hacia un servidor L2F (un Router). L2F funciona sólo en túneles obligatorios.

2.8.4 Protocolo de túnel de nivel 2 (L2TP)

L2TP es una combinación del PPTP y L2F. Sus diseñadores esperan que el L2TP represente las mejores funciones del PPTP y L2F.

L2TP es un protocolo de red que encapsula las tramas del PPP que se enviarán sobre redes IP, X.25, Frame Relay o ATM. L2TP se puede utilizar como un protocolo de túnel sobre Internet. También se puede utilizar al L2TP directamente sobre varios medios WAN (como Frame Relay) sin nivel de transporte IP.

El L2TP sobre las redes IP utilizan UDP y una serie de mensajes del L2TP para el mantenimiento del túnel. El L2TP también utiliza UDP para enviar tramas del PPP. Se pueden encriptar y/o comprimir las cargas útiles de las tramas PPP encapsuladas.

2.8.5 PPTP comparado con L2TP

Tanto el PPTP como L2TP utilizan el PPP para proporcionar una envoltura inicial de los datos y luego incluir encabezados adicionales para transportarlos a través de la red. Los dos protocolos son muy similares. Sin embargo, existen diferencias entre el PPTP y L2TP:

• El PPTP requiere que la red sea de tipo IP. El L2TP requiere sólo que los medios del túnel proporcionen una conectividad de punto a punto orientada a paquetes. Se puede utilizar L2TP sobre IP (utilizando UDP), circuitos virtuales permanentes, circuitos virtuales X.25 o ATM.

• L2TP proporciona la autenticación de túnel, mientras que el PPTP no. Sin embargo, cuando se utiliza cualquiera de los protocolos sobre IPSec, se proporciona la autenticación de túnel por el IPSec de tal manera que no sea necesaria la autenticación del túnel Nivel 2.

2.8.6 Protocolo de seguridad de Internet (IPSEC)

El IPSec es un estándar de protocolo de Nivel 3 que da soporte a la transferencia protegida de información a través de una red IP. Además de su definición de mecanismos de encriptación para tráfico IP, IPSec define el formato de paquete para un modo de túnel IP sobre IP. Un túnel IPSec

consiste en un cliente de túnel y un servidor de túnel y un mecanismo negociado de encriptación.

Se puede usar cualquier protocolo IP sobre IPSec. La forma en la que se configuran los sistemas IPSec, es hasta un cierto punto, trabajo del diseñador; sin embargo, el RFC (manual de seguridad de redes) contiene algunas recomendaciones importantes sobre cómo se debería implementar.

Finalmente, un componente clave en la seguridad de la VPN es el manejo de la autenticación y autorización a usuarios para el acceso a los recursos de la red corporativa. Para esto se utilizan servidores de AAA (autenticación, autorización y contabilidad) a los cuales se accede mediante los protocolos RADIUS o TACACS.

2.9 TIPOS DE TÚNEL

Se pueden crear túneles en diferentes formas.

• Túneles voluntarios*:* Una computadora de usuario o de cliente puede emitir una solicitud VPN para configurar y crear un túnel voluntario. En este caso, la computadora del usuario es un punto terminal del túnel y actúa como un cliente del túnel.

• Túneles obligatorios: Un servidor de acceso de marcación capaz de soportar una VPN configura y crea un túnel obligatorio. Con un túnel obligatorio, la computadora del usuario deja de ser un punto terminal del túnel. Otro dispositivo, el servidor de acceso remoto, entre la computadora del usuario y el servidor del túnel, es el punto terminal del túnel y actúa como el cliente del túnel.

FEP es el servidor que deberá tener instalado el protocolo apropiado de túnel y deberá ser capaz de establecer el túnel cuando se conecte la computadora cliente.

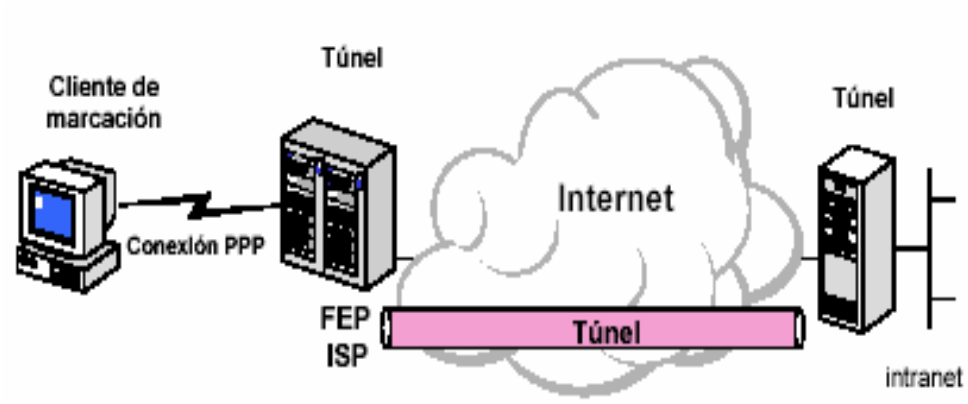


Figura 2.7 Túneles obligatorios

2.10 PRODUCTOS QUE SOPORTAN VPN

2.10.1 Dispositivos

- ✓ Router Multiservicio Modular de la serie Cisco 2600

Figura 2.8 Router Cisco 2600 Series

La serie Cisco 2600, ofrece una solución rentable para satisfacer las necesidades actuales y futuras de las sucursales en lo referente a:

- Integración multiservicio de voz y datos
- Acceso a redes privadas virtuales (VPN) con opciones de firewall
- Servicios de acceso telefónico analógico y digital
- Enrutamiento con gestión de ancho de banda
- Enrutamiento entre VLAN

Permite aplicar funciones de seguridad tales como el cifrado de datos, tunneling y autenticación y autorización de usuarios para acceder a la VPN

Permite el enrutamiento entre VLAN a través del protocolo ISL (Inter-Switch Link)

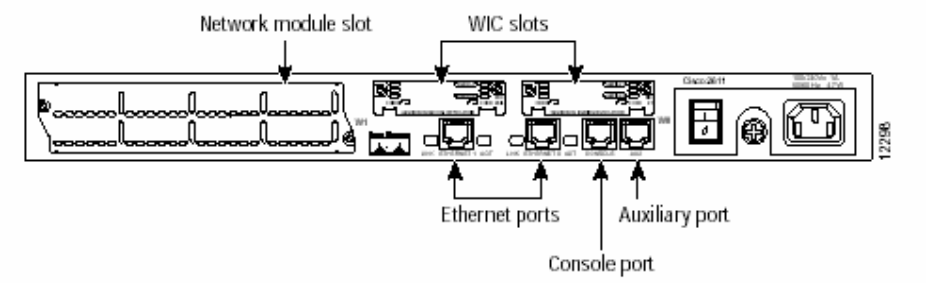


Figura 2.9 Puertos del Router

✓ Cisco Catalyst 6500 Series

Figura 2.10 Cisco Catalyst 6500 Series

El Switch Catalyst de la serie 6500 de cisco, cuenta con módulo de Firewall ideal para centros de datos, Extranet, seguridad en aplicaciones Web, etc. Ademas, posee un modulo IPSec para servicios de VPN.

- ✓ Familia SuperStack II NETBuilder SI (3Com)

Figura 2.11 SuperStack II NETBuilder SI (3Com)

• Características

Este Router incorpora funciones de cifrado IPSec.

Cuenta con el software Quick Step VPN, una interfaz basada en navegador, muy fácil de utilizar, que permite configurar túneles de VPN.

Además, la tecnología de VPN de 3Com se basa en protocolos estándar, como el protocolo de tunelización punto a punto (PPTP) y el protocolo de tunelización de nivel 2 (L2TP), que garantizan la máxima interoperatividad en distintos entornos.

✓ Concentrado Cisco VPN 5001

Figura 2.12 Concentrador Cisco VPN 5001

El concentrador Cisco VPN 5001 es un flexible dispositivo para las instalaciones de los clientes diseñado para afrontar las demandas de los servicios basados en redes virtuales privadas (VPN) tanto de acceso remoto como de ubicación a ubicación. Esta plataforma incorpora avanzadas capacidades de cifrado y autenticación de alto rendimiento.

Características	Ventajas
Compatibilidad con varios protocolos: IP o IPX para VPN de cliente a ubicación, IP, IPX y AppleTalk para VPN de ubicación a ubicación (sólo con concentradores VPN 5000 en ambos extremos)	Esto permite que las empresas utilicen la infraestructura de propiedad IPX y AppleTalk existente para las VPN
Capacidad de ampliación y rendimiento • Permite hasta 1.500 túneles	Permite que las oficinas remotas puedan crecer sin sustituir el concentrador VPN.

• Proporciona 50 Mbps • Cualquier combinación de IPSec, L2TP o PPP	
Clientes para Windows, MacOS, Sun Solares y Linux	Proporciona la más amplia compatibilidad con las plataformas de clientes del mercado, lo que permite a los usuarios acceder a sus VPN prácticamente desde cualquier plataforma de estación de trabajo.

Tabla 2.1 Características y ventajas del Concentrador Cisco VPN 5001

2.10.2 Productos

- F-Secure VPN

Es una solución flexible y de coste aprovechable para obtener los beneficios de Internet comprometiéndose a mantener la seguridad. Es mejor usar este

paquete en unión a un Firewall para conseguir un control total sobre el tráfico de datos de toda la organización.

F-Secure VPN es un producto comercial de la compañía Data Fellows que se encuentra dentro de la línea de productos enfocados a la seguridad de Internet. Usa los mecanismos de encriptación disponibles, más sofisticados y además es compatible con las arquitecturas modernas Cliente-Servidor y por supuesto Internet.

Las características principales son las siguientes:

Fácil de instalar: Requiere muy pocos parámetros de instalación para el administrador, durante la instalación inicial.

Fácil de configurar: F-Secure VPN destaca por un editor de red gráfico que permite configurar la totalidad de la red VPN desde una simple estación de trabajo.

Configurable para asegurar las conexiones Extranet: Con el editor de red de F-Secure VPN, se puede definir la seguridad en las conexiones Extranet con los clientes habituales.

Seguro: Usa una extensa variedad de algoritmos de selección de usuarios, incluyendo 3DES, Blowfish, IKE, Firmas RSA, Certificado X.509, etc.

Disponible a nivel global, con una fuerte encriptación: Data Fellows puede enviar el software encriptado a todo el mundo, sin ningún compromiso, desde las oficinas situadas en Colombia o Europa.

- IPSec Express

  Producto comercial

  Autenticación: HMAC-MD5-96, HMAC-SHA1-96, DES-MAC.

  Cifrado: 3DES, Blowfish.

  Intercambio de caves: IKE, Firmas RSA, Certificado X.509

- Free S/WAN

  Libre distribución

  Autenticación: HMAC-MD5, HMAC-SHA1.

  Cifrado: 3DES.

  Intercambio de caves: IKE.

- Otros dispositivos

  - VTCP/Secure (InfoExpress)

  - AltaVista Tunnel (DEC)

  - Smartgate (V-One)

  - TunnelBuilder (Network TeleSystem)

- MovileVPN (Aventail)

- PPTP (Microsoft)

2.10.3 Software IOS para la serie cisco

Proporciona una funcionalidad, estabilidad y seguridad comunes para todos los productos que estén bajo la arquitectura CiscoFusión. El software IOS permite la instalación y administración centralizada, integrada y automatizada de *internetworks,* garantizando soporte a una amplia gama de protocolos, medios, servicios y plataformas.

Software Cisco IOS c2600-i-mz, Version 12.2(2) XA5 para la serie Cisco 2600:

La serie Cisco 2600 (Cisco 2610, Cisco 2611, Cisco 2612, Cisco 2613, Cisco 2620 y 2621, Cisco 2650 y 2651) ofrece grupos de características Plus, de cifrado y Firewall.

Los conjuntos básicos de características admiten los protocolos y estándares más utilizados, tales como NAT, OSPF, BGP, RADIUS (Remote Access Dial-In User Service), IP Multicast, RMON y las características de optimización de WAN (como ancho de banda bajo demanda, gestión de colas personalizada, por prioridades y ponderada, acceso telefónico de respaldo y RSVP).

El software IOS de Cisco ofrece las siguientes características:

• Plus con IPSec Encryption (de 56 bits y 168 bits con 3DES)

• Firewall Plus

• Plus con cifrado y Firewall

Los conjuntos de características Plus contienen: L2TP, L2F, VLAN, etc. Otros conjuntos de características incluyen cifrado IPSec y 3DES, así como capacidades de firewall certificadas ICSA con detección de intrusiones.

Data Encryption AIM para la serie Cisco 2600 requiere el software IOS, versión 12.1(3)XI o superior.

Nombre de la imagen (Image Name)	Software de la imagen (Software Image)
IP Plus	c2600-is-mz
IP Plus IPsec 3DES	c2600-ik9s-mz
IP Plus IPsec 56	c2600-ik8s-mz
IP/FW/IDS Plus IPsec 3DES	c2600-ik9o3s-mz
IP/FW/IDS Plus IPsec 56	c2600-ik8o3s-mz
Enterprise Plus IPsec 3DES	c2600-jk9s-mz

Enterprise Plus IPsec 56	c2600-jk8s-mz
Enterprise/FW/IDS Plus IPsec 3DES	c2600-jk9o3s-mz
Enterprise/FW/IDS Plus IPsec 56	c2600-jk8o3s-mz
Enterprise/SNASw Plus IPsec 3DES	c2600-a3jk9s-mz
Enterprise/SNASw Plus IPsec 56	c2600-a3jk8s-mz

PRÁCTICAS DE LABORATORIO

3. DISPOSITIVOS DE REDES

3.1 HUB

Las redes locales Ethernet originales fueron creadas llevando cables entre edificios y conectando cada estación punto a punto.

Los Hubs han evolucionado en varias generaciones desde los primeros y simples Hubs repetidores. Ahora son componentes en los sistemas de cableado estructurado que soportan muchas topologías de redes locales y de gran alcance.

Figura 3.1 Hubs

Los Hubs se hicieron populares en el entorno de redes locales con el desarrollo de topologías 10Base-T configuradas en estrella. Hay grandes redes desarrolladas con muchos de estos Hubs, conectados entre sí para formar redes departamentales e interconexiones de redes.

3.1.1 Definición de Hub

Los Hubs simples son dispositivos concentradores a los cuales pueden conectarse varias estaciones y servidores. Ethernet 10Base-T utiliza Hubs como repetidores de señal entre las estaciones conectadas, y le permite crear una topología en estrella.

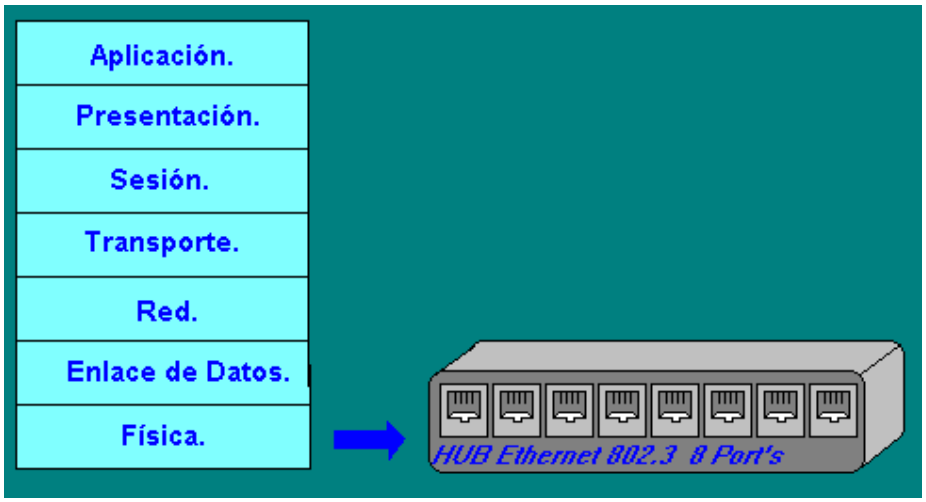


Figura 3.2 Hub en la capa física del modelo OSI

Los Hubs forman el enlace central de los sistemas de cableado estructurado tal como muestra la siguiente figura, donde se observa una configuración lógica y física.

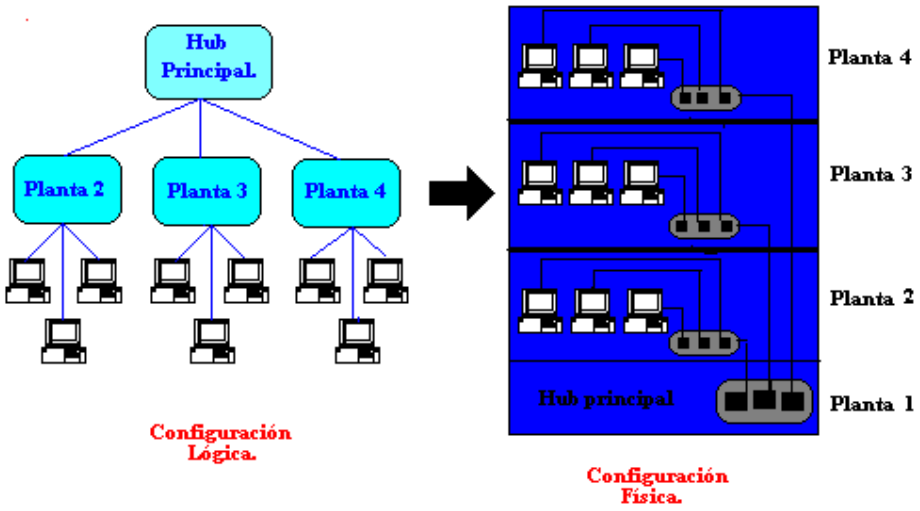


Figura 3.3 Configuración lógica y física

El propósito de un Hub es regenerar y reenviar señales de red a nivel de bits. Los Hubs se utilizan por dos razones: para crear un punto de conexión central para los medios de cableado y para aumentar la confiabilidad de la red.

Figura 3.4 Hub estándar de Cisco

3.1.2 Características de los Hubs

- Los Hubs ayudan a las empresas a gestionar el crecimiento de sus redes. Generalmente forman los enlaces centrales de los sistemas de cableado estructurado para facilitar la planificación del crecimiento futuro.
- Un Hub típico de empresa podrá acomodar muchos tipos de redes diferentes, incluyendo Ethernet, Token Ring, FDDI, o conexiones de redes de gran alcance, como Frame Relay, ATM, etc.
- Un Hub puede servir como centro de conexiones para toda una planta, un edificio, un campus, o incluso una red global.
- El Hub también se denomina repetidor multipuesto.
- Los Hubs se consideran dispositivos de Capa 1 dado que sólo regeneran la señal y la envían por medio de un Broadcast a todos los puertos (conexiones de red).

3.1.3 Clasificación de los Hubs

Podemos clasificar los Hubs en tres grupos principales, basándonos en cómo se utilizan en un sistema de cableado estructurado:

- Hub de grupo de trabajo: Un Hub de grupo de trabajo conecta un grupo de equipos que se encuentran en sus cercanías. Por Ejemplo, podría conectar 8 computadoras del departamento de diseño.
- Hubs intermedios: Un Hub intermedio se encuentra generalmente en una pequeña central de conexiones situada en cada planta. Los Hubs de grupo de trabajo son conectados a ésta, que a su vez está

conectado al Hub de la empresa. El tráfico entre los Hubs de grupos de trabajos locales puede ser gestionados por el Hub intermedio o bien por el Hub de empresa, el cual puede gestionar todo el tráfico de la interconexión de redes, dependiendo de sus necesidades o el diseño de los Hubs.

- Hub de empresa: El Hub de empresa es el punto de conexión central para todos los sistemas finales conectados a grupos de trabajo. Los Hubs de empresa forman el propio Backbone u ofrecen conexiones a un Backbone. Pueden ofrecer Bridges, encaminamiento y servicios de conexiones de gran alcance.

Otra clasificación de los Hubs corresponde a Hubs inteligentes y Hubs no inteligentes. Los Hubs inteligentes tienen puertos de consola, lo que significa que se pueden programar para administrar el tráfico de red. Los Hubs no inteligentes simplemente toman una señal de Networking entrante y la repiten hacia cada uno de los puertos sin la capacidad de realizar ninguna administración.

3.1.4 Especificaciones de los Hubs de la CUTB

- Hub # 1

  3 COM Super Stack II - Hub 10

  Código de inventario en la CUTB: 23845

- Hub # 2

  3 COM Super Stack II - Baseline Hub - 3C 16441

  Código de inventario en la CUTB: 28516

- Hub # 3

  3 COM Super Stack II - Baseline Hub - 3C 16441

  Código de inventario en la CUTB: 22216

3.2 SWITCH

Figura 3.5 Switch estándar de Cisco

En el gráfico se indica el símbolo que corresponde al Switch. Las flechas de la parte superior representan las rutas individuales que pueden tomar los datos en un Switch, a diferencia del Hub, donde los datos fluyen por todas las rutas.

3.2.1 Definición de Switch

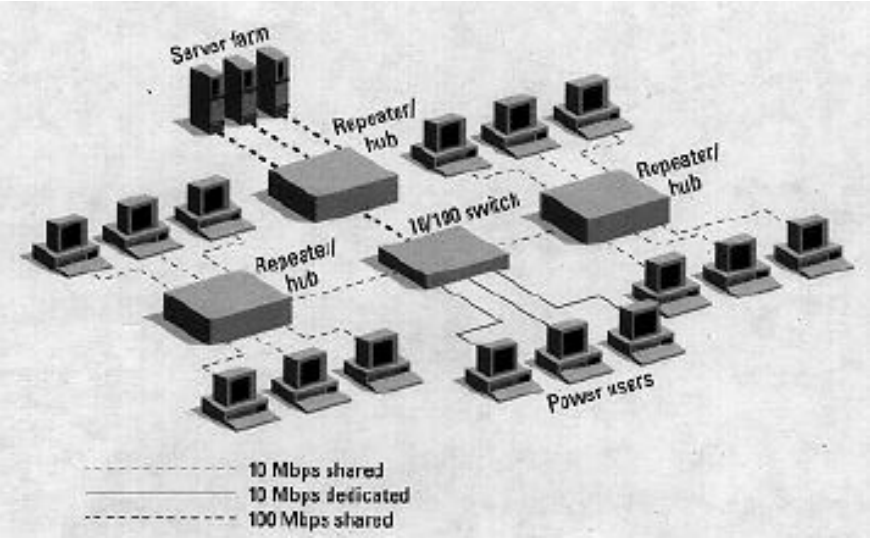


Figura 3.6 Red segmentada con Switch

El propósito del Switch es concentrar la conectividad, haciendo que la transmisión de datos sea más eficiente.

El Switch conmuta paquetes desde los puertos (interfaces) entrantes a los puertos salientes, suministrando a cada puerto el ancho de banda total (la velocidad de transmisión de datos en el Backbone de la red).

3.2.2 Características de los Switch

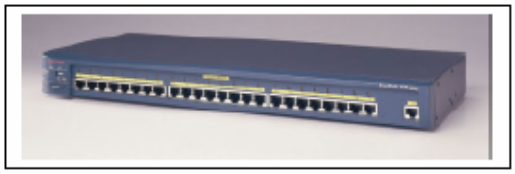


Figura 3.7 Switch

- La tecnología de Switches opera en su mayoría, en la capa 2 del modelo OSI.
- El Switch toma decisiones de envío relativamente sencillas basándose en la dirección MAC de destino contenida en cada paquete y, generalmente, sin tomar en consideración otros datos incluidos en esté.
- Puede reenviar los datos con periodos de latencia muy bajos, proporcionando así un rendimiento próximo al de un solo segmento de LAN.
- La creciente popularidad de los Switches podría interpretarse como el resurgimiento de la tecnología de Bridge en un dispositivo más sencillo y más económicos con mejores prestaciones y mayor cantidad de puertos.
- La tecnología de Switches permite incrementar el ancho de banda tanto en segmentos de LAN compartidos como dedicados y elimina los cuellos de botella entre varias LAN.
- En la actualidad los productos de Switches se encuentran disponibles para todas las tecnologías (Ethernet, Fast Ethernet, FDDI, ATM y Token Ring).

- Los Switches ofrecen grandes ventajas en el ámbito de la interconectividad ya que segmentan la red en dominios de colisión más pequeños proporcionando mayor porcentaje de ancho de banda para cada estación. Su transparencia en el soporte de protocolos permite instalarlos en redes multiprotocolos con escasa o ninguna configuración de software.
- Los Switches utilizan el cableado existente, los Hubs y los adaptadores del puesto de trabajo prácticamente sin necesidad de efectuar inversiones en hardware. Por último, su total transparencia con respecto a la estación de trabajo final reduce el trabajo administrativo simplificando las operaciones de traslados y modificaciones dentro de la red.

3.2.3 El futuro de los Switch

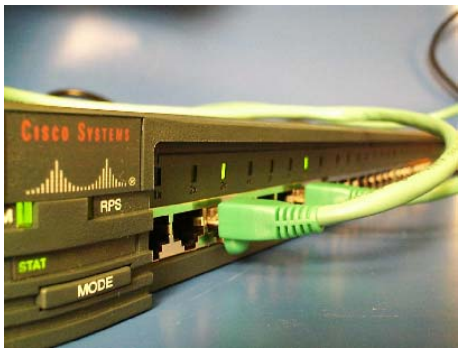


Figura 3.8 Switch Cisco

El precio de la tecnología del Switch continúa descendiendo. Como el costo por puerto del Switch se aproxima al de los Hubs, muchos usuarios eligen el Switch.

La extensa disponibilidad de la tecnología de Switch de bajo costo tiene implicaciones para las redes de los edificios y el Backbone de campus. Habrá una demanda creciente para Switches de Backbone de alta densidad, con un número grande de puertos de alta velocidad, para enlazar grupos de trabajo individuales.

Eventualmente el equipo de escritorio será dedicado a enlaces de 10 Mbps, la mayoría de los servidores estarán conectados a los Switch de alta velocidad y ATM se usará en enlaces internos del edificio y al Backbone de campus.

Un buen despliegue de aplicaciones multimedia requiere que la red tenga altos niveles de funcionalidad y calidad fija en el servicio. Hay diversas innovaciones que se integran dentro de la tecnología del Switch para realzar el soporte de futuras aplicaciones multimedia.

3.2.4 Especificaciones de los Switch de la CUTB

- Switch #1

  CATALYST 2950 Series

  Código de inventario en la CUTB: 35364

Version: C 2950 Boot loader (C2950–HBOOT-M) versión 12.1 (0,0.49) EA2

Flash: C2950-C3h2s-mz.120-5.3.wc.1.bin

IOS (tm) C2950 Software (C2950-C3H 25-M)

IOS Version 12.0 (5.3) WC (1)

Directory of flash:/ 6 -rwx 660 Vlan.dat

Cisco WS-C2950-12 (RS 32300) Proccessor (revision CO)

12 fast Ethernet

- Switch #2

  CATALYST 2900 Series XL

  Código de inventario en la CUTB: 35370

  Version: C2900 XL Boot loader (C2900–HBOOT-M) versión 12.0 (5,3) WC(1)

  IOS Version 12.0 (5) WC 3b

  24 fast Ethernet

3.3 ROUTER

El propósito de un Router es examinar los paquetes entrantes (datos de capa 3), elegir cuál es la mejor ruta para ellos a través de la red y luego conmutarlos hacia el puerto de salida adecuado.

3.3.1 Definición de Router

Los routers son los dispositivos de regulación de tráfico más importantes en las redes. Permiten que prácticamente cualquier tipo de computador se pueda comunicar con otro computador en cualquier parte del mundo.

El Router esta diseñado para segmentar la red, con la idea de limitar tráfico de Broadcast y proporcionar seguridad, control y redundancia entre dominios individuales de Broadcast, también puede dar servicio de Firewall y un acceso económico a una WAN.

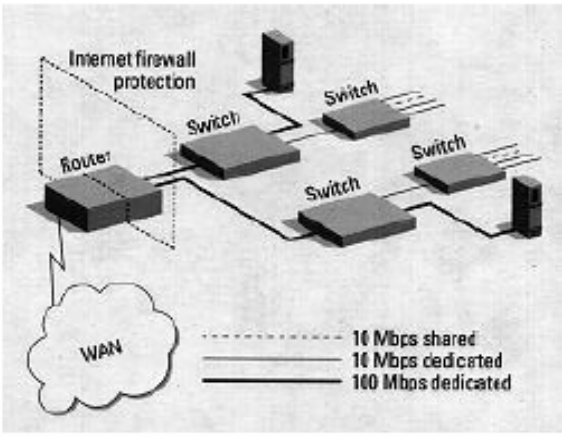


Figura 3.9 Segmentación de red con Router

3.3.2 Características de los Routers

- Los Router permiten, enlazar redes con protocolos distintos: IP, IPX, AppleTalk, DECnet

- Proporcionar seguridad a través de sofisticados filtros de paquetes, en ambiente LAN y WAN.

- Permitir diseñar redes jerárquicas, que deleguen autoridad y puedan forzar el manejo local de regiones separadas de redes internas.

- Integrar diferentes tecnologías de enlace de datos, tales como Ethernet, Fast Ethernet, Token Ring, FDDI y ATM.

3.3.3 Funcionamiento de los Routers

Figura 3.10 Router estándar de Cisco

- Un Router examina la información de encaminamiento de los paquetes y los dirige al segmento de red adecuado.

- Si el Router está en un servidor, envía los paquetes destinados para ese servidor a los protocolos de niveles superiores.

- Un Router solo procesa los paquetes que van dirigidos a él, lo que incluye a los paquetes enviados a otros routers con los que esté conectado.

- Los routers envían los paquetes por la mejor ruta hacia su destino. Mantienen tablas de redes locales y routers adyacentes en la red.

- Cuando un Router recibe un paquete, consulta estas tablas para ver si puede enviar directamente el paquete a su destino. Si no es así, determina la posición de un Router que pueda enviar el paquete a su destino.

- Los Routers permiten dividir una red en redes lógicas. Estas redes lógicas son más sencillas de manejar. Cada segmento de red tiene su

propio número de red local, y cada estación de dicho segmento tiene su propia dirección.

3.3.4 Futuro de los Routers

El Router es la llave para desarrollar redes internas. El desafío es integrar el Switch con Router para que el sistema aproveche el diseño de la red. Inicialmente los Switches estarán en todas las organizaciones que requieran incrementar el ancho de banda y obtener la funcionalidad que necesitan. No obstante al incrementar la complejidad de la red, los administradores necesitarán controlar el ambiente de Switch, usando segmentación, redundancia, Firewall y seguridad. El usuario demandará que los vendedores de Routers hagan sus productos fáciles de instalar y configurar.

3.3.5 Principales comandos y modos del Router

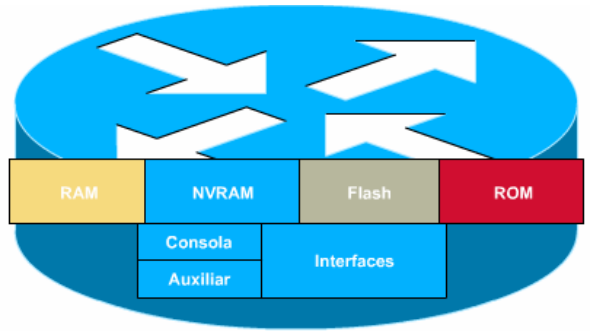


Figura 3.11 Memorias y modos del Router

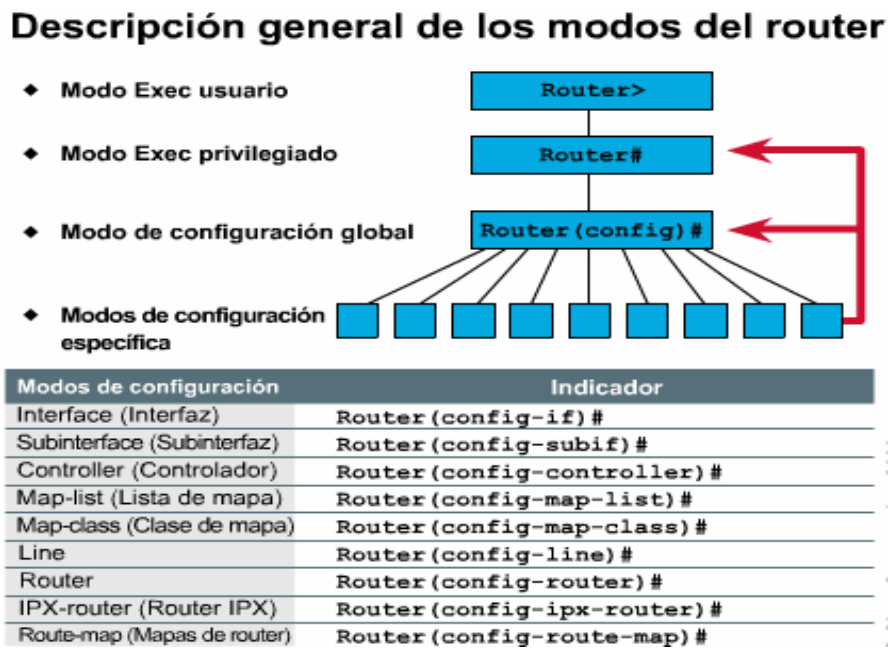
- **show version**: Muestra la configuración del hardware del sistema, la versión del software, los nombres y orígenes de los archivos de configuración y la imagen de arranque.
- **show processes**: Muestra información acerca de los procesos activos.
- **show protocols**: Muestra el estado de todos los protocolos configurados de Capa 3.
- **show memory**: Muestra estadísticas acerca de la memoria del Router, incluyendo estadísticas de memoria disponible.
- **show stacks**: Monitorea el uso de la pila de procesos y rutinas de interrupción y muestra la causa del último re-arranque del sistema.
- **show buffers**: Suministra estadísticas sobre los grupos de búfer en el router.
- **show flash**: Muestra información acerca del dispositivo de memoria Flash.
- **show running-config**: Muestra el archivo de configuración activo o muestra la configuración actual en la RAM.
- **show startup-config**: Muestra la copia de respaldo del archivo de configuración. Muestra en pantalla la configuración guardada, que es el contenido de la NVRAM.
- **show interfaces**: Muestra estadísticas para todas las interfaces configuradas en el Router.
- **reload** (reboot): Vuelve a cargar el Router, haciéndolo pasar por todo el proceso de inicio.

- **Setup**: Se usa para entrar en el modo de configuración inicial (setup) desde el indicador EXEC privilegiado.
- **configure terminal**: Realiza la configuración desde la terminal de consola de forma manual.
- **configure memory**: Carga la información de configuración desde la NVRAM.
- **copy tftp running-config**: Carga la información de configuración desde un servidor de red TFTP en la RAM.
- **copy running-config startup-config**: almacena la configuración actual desde la RAM en la NVRAM.
- **copy running-config tftp**: Guarda la configuración actual de la RAM en un servidor de red TFTP.
- **erase startup-config**: Borra el contenido de la NVRAM.
- **ip ardes**: Establece la dirección de red lógica de una interfaz.
- **ip netmask-format**: Especifica el formato de las máscaras de red para la sesión actual.
- **ip host**: Crea una entrada estática que relaciona el nombre de host con la dirección del mismo en el archivo de configuración del Router.
- **ip name-server**: Define cuáles son los Hosts que pueden suministrar el servicio de denominación.
- **show Hosts**: Visualizar una lista en la memoria caché de nombres y direcciones de host.
- **Telnet**: Verifica el software de la capa de aplicación entre las estaciones origen y destino. Es el mecanismo de verificación más completo disponible.

- **ping**: Utiliza el protocolo ICMP para verificar la conexión de hardware y la dirección lógica en la capa de internet. Es un mecanismo de verificación sumamente básico.
- **trace route**: Utiliza valores TTL para generar mensajes desde cada Router que se utiliza a lo largo de la ruta. Es sumamente poderoso en cuanto a su capacidad para ubicar fallas en la ruta desde el origen hasta el destino.
- **ip default-network**: Establece una ruta por defecto en las redes que utilizan protocolos de enrutamiento dinámico.
- **Router**: Inicia el proceso de enrutamiento.
- **network**: Permite que el proceso de enrutamiento pueda determinar cuáles son las interfaces que participarán en el envío y la recepción de actualizaciones de enrutamiento.
- **router rip**: Selecciona a RIP como el protocolo de enrutamiento.
- **show ip protocol**: muestra valores acerca de temporizadores de enrutamiento e información de red, asociados con todo el Router.
- **show ip route**: Muestra el contenido de la tabla de enrutamiento IP, que contiene entradas para todas las redes y subredes conocidas, junto con un código que indica de qué manera se obtuvo la información.
- **router igrp**: Selecciona a IGRP como el protocolo de enrutamiento.
- **show ip protocol**: Muestra parámetros, filtros e información de red acerca de todos los protocolos de enrutamiento (es decir, RIP, IGRP, etc.) en uso en el Router.

- **show ip interfaces**: Muestra el estado y los parámetros globales asociados con todas las interfaces IP.
- **debug ip rip**: Muestra las actualizaciones de enrutamiento RIP a medida que se envían y reciben.

- **Bandwidth**: La capacidad que tiene un medio para transportar datos, usualmente medida en bits por segundos (bps). Se necesita para calcular el tiempo muerto entre petición y petición. El sistema de ancho de banda bajo demanda (Bandwidth-on-Demand, BOD) es otra importante función que permite que los usuarios de ISDN (RDSI) agreguen dinámicamente múltiples canales B para obtener un mayor ancho de banda cuando sea necesario Ancho de Banda, Bandwidth diferencia entre la frecuencia de banda más alta y más baja.



Modos de configuración	Indicador
Interface (Interfaz)	Router(config-if)#
Subinterface (Subinterfaz)	Router(config-subif)#
Controller (Controlador)	Router(config-controller)#
Map-list (Lista de mapa)	Router(config-map-list)#
Map-class (Clase de mapa)	Router(config-map-class)#
Line	Router(config-line)#
Router	Router(config-router)#
IPX-router (Router IPX)	Router(config-ipx-router)#
Route-map (Mapas de router)	Router(config-route-map)#

Figura 3.12 Modos del Router

3.3.6 Métodos de configuración de contraseñas

Se puede garantizar la seguridad del sistema utilizando contraseñas para restringir el acceso. Las contraseñas se pueden establecer tanto en líneas individuales como en el modo EXEC privilegiado.

- line console 0: establece una contraseña en la terminal de consola
- line vty 0 4: establece protección mediante contraseña en las sesiones Telnet entrantes
- enable password: restringe el acceso al modo EXEC privilegiado
- enable secret: password (del diálogo de configuración del sistema para establecer parámetros globales): utiliza un proceso de cifrado propietario de Cisco para modificar la cadena de caracteres de la contraseña

Puede además evitar que las contraseñas se visualicen utilizando el comando service password-encryption. Este algoritmo de cifrado no coincide con el Estándar de Cifrado de Datos (DES).

3.3.7 Diferencia entre Hubs, Switches y Routers

- El Router tiene más facilidades de software que un Switch. Al funcionar en una capa mayor que la del Switch, el Router distingue entre los diferentes protocolos de red, tales como IP, IPX, AppleTalk o DECnet. Esto le permite hacer una decisión más inteligente que al Switch, al momento de reenviar los paquetes.

- Los Switches toman decisiones basadas en direcciones MAC o físicas, los Router toman decisiones basadas en direcciones de red y los Hub no toman decisiones.

3.3.8 Especificaciones de los Routers de la CUTB

- Router #1

  CISCO 2600 Series

  Código de inventario en la CUTB: 35342

  Cisco 2620 (MPC 860) Proccessor

  IOS (tm) C2600 Software (C2600-D-M)

  Version: 12.1 (8c), Release Software (fc1)

  IOS C2600-d-mz.121-8c.bin

  1 fast Ethernet

  Seriales network Interfaces

- Router #2

  CISCO 2600 Series

  Código de inventario en la CUTB: 35339

  Cisco 2620 (MPC 860) Proccessor

  IOS (tm) C2600 Software (C2600-D-M)

  Version: 12.1 (8c), Release Software (fc1)

  IOS C2600-d-mz.121-8c.bin

  1 fast Ethernet

  2 Seriales network Interfaces

- Router #3

  CISCO 2600 Series

  Código de inventario en la CUTB: 35343

  Cisco 2621 (MPC 860) Proccessor

  IOS (tm) C2600 Software (C2600-D-M)

  Version: 12.1 (8c), Release Software (fc1)

  IOS C2600-d-mz.121-8c.bin

  1 fast Ethernet

  2 Seriales network Interfaces

- Router #4

  CISCO 2600 Series

  Código de inventario en la CUTB: no tiene

  Cisco 2620 (MPC 860) Proccessor

  IOS (tm) C2600 Software (C2600-D-M)

Version: 12.1 (8c), Release Software (fc1)

IOS C2600-d-mz.121-8c.bin

1 fast Ethernet

2 Seriales network Interfaces

- Router #5

  CISCO 2600 Series

  Código de inventario en la CUTB: 35341

  Cisco 2620 (MPC 860) Proccessor

  IOS (tm) C2600 Software (C2600-D-M)

  Version: 12.1 (8c), Release Software (fc1)

  IOS C2600-d-mz.121-8c.bin

  1 fast Ethernet y 2 Seriales network Interfaces

4. PRÁCTICAS DE V-LAN

4.1 PRÁCTICA DE V-LAN POR PUERTO CON UN SWITCH

Duración estimada: 45 min.

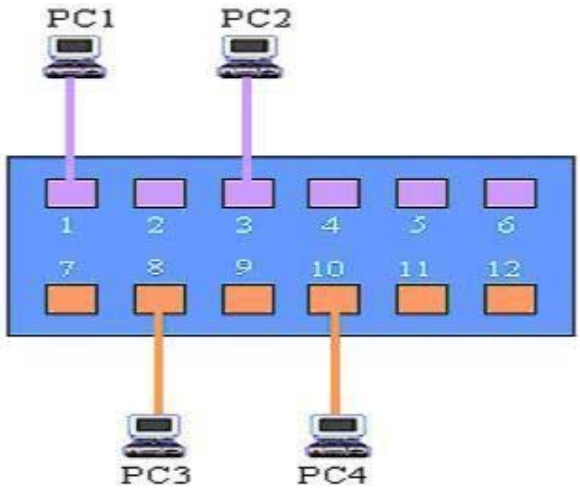


Figura 4.1 V-LAN con un Switch

Nombre del Switch 1 : SW-1
Tipo de Switch : 2950
Nombre de V-LAN1 : alumnos
Nombre de V-LAN2 : profesores
Puertos para V_LAN1 : 1,2,3,4,5 y 6
Puertos para V_LAN2 : 7,8,9,10,11 y 12
IP de los PCs de la V-LAN1 : 172.20.40.(3-8) 255.255.252.0 Puerta de enlace : 172.20.40.1
IP de los PCs de la V-LAN2 : 172.20.44.(3-8) 255.255.252.0 Puerta de enlace : 172.20.44.1

LEYENDA

 = Switch

 = usuarios

= V-LAN1 (alumnos)

= V-LAN2 (profesores)

4.1.1 Objetivos

Esta práctica de laboratorio sirve para practicar las siguientes tareas:

- Conectarse a través de la consola al Switch para crear o configurar 2 V-LANs con sus respectivos nombres
- Configurar cada puerto del Switch a una V-LAN especifica para probar o hacer ping entre cada uno de los Host conectados a cada VLAN

4.1.2 Información básica

En esta práctica de laboratorio se trabaja con redes de área local virtuales de Ethernet (VLAN). Las VLAN se pueden usar para separar grupos de usuarios según la función en lugar de la ubicación física. Normalmente todos los puertos en un Switch están en la misma VLAN 1 por defecto. En esta práctica implementaremos las V-LANs por puerto, donde cada puerto del Switch puede asociarse a una VLAN. Un administrador de red puede crear VLAN adicionales y desplazar algunos puertos a los de las VLAN para

crear grupos aislados de usuarios sin importar dónde se ubican físicamente. Esto crea dominios de broadcast más pequeños que ayudan a reducir y localizar el tráfico de red. Si un Switch con 12 puertos se divide en 2 VLAN de 6 puertos cada uno, los usuarios de una VLAN no podrán acceder a los recursos (como servidores o impresoras) en la otra VLAN.

Accederá mediante la consola al Switch para administrar las VLAN. Esta práctica de laboratorio ayudará a demostrar cómo las VLAN se pueden usar para separar el tráfico y reducir los dominios de broadcast.

4.1.3 Herramientas / preparación

Antes de comenzar con la práctica de laboratorio, el profesor o asistente de laboratorio debe preparar un Switch con los valores VLAN por defecto. Se debe colocar también a disposición una estación de trabajo con HyperTerminal para realizar la conexión de consola al Switch. A continuación se suministra la lista de equipo requerido.

- Un estación de PC con HyperTerminal instalado para configurar el Switch
- Cuatro estaciones de PC Windows
- Switch Cisco (modelo 2900 Series)
- Cable de consola (roll-over) y adaptador DB-9/RJ45 o cable de módem nulo DB-9
- Cable Ethernet CAT 6 desde cada estación de trabajo a un puerto Ethernet de switch

4.1.4 Recursos web

- LAN Switching basics
  www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/lanswtch.htm
- General information on all Cisco products - (Ir al capítulo 22 - Switches) www.cisco.com/univercd/cc/td/doc/pcat/#2
- 1900 / 2820 series Ethernet switches
  www.cisco.com/warp/public/cc/pd/si/casi/ca1900/prodlit/s1928_ov.htm
- 2900 series Fast Ethernet switches
  www.cisco.com/warp/public/cc/pd/si/casi/ca2900xl/prodlit/s290xl_ov.htm
- 3500 series Gigabit Ethernet switches
  www.cisco.com/warp/public/cc/pd/si/casi/ca3500/prodlit/s3500x_ov.htm
- Virtual LAN for 1900/2820 Switches
  www.cisco.com/univercd/cc/td/doc/product/lan/28201900/1928v8x/eesc98x/02vlans.htm

4.1.5 Notas

4.1.6 Comandos a utilizar en la práctica de V-LAN por puerto con un Switch

Comandos	Descripción
configure terminal	Entra al modo de configuración global. Realiza la configuración desde la terminal de consola de forma manual
End	Sale del modo de configuración
interface fastEthernet 0/id	Entra a una interface FastEthernet establecidas por el usuario
Ping	Utiliza el protocolo ICMP para verificar la conexión de hardware y la dirección lógica en la capa de internet, envía mensajes de eco al dispositivo vecino
Show running-config	Muestra el archivo de configuración activo o muestra la configuración actual en la RAM
Show vlan	Muestra todas la V-LANs con sus respectivos puertos asignados a cada una de ellas

switchport mode access vlan id	Asigna un puerto a una V-LAN
vlan database	Entra al modo de configuración de las VLAN

Tabla 4.1 Comandos de la práctica de V-LAN con un Switch

4.1.7 Pasos para la práctica de V-LAN por puerto con un Switch

Seleccione un Switch que tenga 12 puertos FastEthernet (modelo Cisco 1900 Series) y 4 PCs antes de comenzar la práctica de Laboratorio. Conecte una estación de trabajo a la conexión del puerto de consola del Switch para configurar cada puerto con su respectiva V-LAN y conecte los 4 computadores al Switch en los puertos 1, 3, 8 y 10.

Paso 1 – Utilizar el diagrama de laboratorio, colocar los siguientes comandos para crear V-LANs y responda las siguientes preguntas:

SW-1# show vlan

1. ¿Cuántos puertos están asignados a la V-LAN 1?

2. ¿Cuántos puertos están asignados a la V-LAN 2?

_____

Paso 2 – Asignar puertos a cada V-LAN con los siguientes comandos y contestar las siguientes preguntas:

SW-1# configure terminal

SW-1(config)# interface fastEthernet 0/7

SW-1(config-if)# switchport mode access vlan 2

SW-1(config-if)# end

SW-1# configure terminal

SW-1(config)# interface fastEthernet 0/8

SW-1(config-if)# switchport mode access vlan 2

SW-1(config-if)# end

SW-1# configure terminal

SW-1(config)# interface fastEthernet 0/9

SW-1(config-if)# switchport mode access vlan 2

SW-1(config-if)# end

SW-1# configure terminal

SW-1(config)# interface fastEthernet 0/10

SW-1(config-if)# switchport mode access vlan 2

SW-1(config-if)# end

SW-1# configure terminal

SW-1(config)# interface fastEthernet 0/11

SW-1(config-if)# switchport mode access vlan 2

SW-1(config-if)# end

SW-1# configure terminal

SW-1(config)# interface fastEthernet 0/12

SW-1(config-if)# switchport mode access vlan 2

SW-1(config-if)# end

SW-1# show running-config

3. ¿Cuántas interfaces FastEthernet están asignadas a la V-LAN 1?

_____

4. ¿ Cuántas interfaces FastEthernet están asignadas a la V-LAN 2?

_____

Paso 3 - Probar la funcionalidad de las 2 VLAN utilice el comando ping en cada estación de trabajo y contestar las siguientes preguntas:

5. Emita un ping del PC1 a las demás estaciones de trabajo. ¿El ping fue exitoso?

_____

_____

6. Cambie el PC1 del puerto 1 al puerto 7 y emita un ping a las demás estaciones. ¿qué ocurrió?

_____

_____

4.1.8 Respuestas de la práctica de V-LAN por puerto con un Switch

Paso 1 – Utilizar el diagrama de laboratorio, colocar los siguientes comandos para crear V-LANs y responda las siguientes preguntas:

SW-1# show vlan

1. ¿Cuántos puertos están asignados a la V-LAN 1?

Todos los puertos pertenecen a la V-LAN 1

2. ¿Cuántos puertos están asignados a la V-LAN 2?

Ninguno, porque no se ha configurado los puertos del Switch para la VLAN 2

Paso 2 – Asignar puertos a cada V-LAN con los siguientes comandos y contestar las siguientes preguntas:

SW-1# configure terminal

SW-1(config)# interface fastEthernet 0/7

SW-1(config-if)# switchport mode access vlan 2

SW-1(config-if)# end

SW-1# configure terminal

SW-1(config)# interface fastEthernet 0/8

SW-1(config-if)# switchport mode access vlan 2

SW-1(config-if)# end

SW-1# configure terminal

SW-1(config)# interface fastEthernet 0/9

SW-1(config-if)# switchport mode access vlan 2

SW-1(config-if)# end

SW-1# configure terminal

SW-1(config)# interface fastEthernet 0/10

SW-1(config-if)# switchport mode access vlan 2

SW-1(config-if)# end

SW-1# configure terminal

SW-1(config)# interface fastEthernet 0/11

SW-1(config-if)# switchport mode access vlan 2

SW-1(config-if)# end

SW-1# configure terminal

SW-1(config)# interface fastEthernet 0/12

SW-1(config-if)# switchport mode access vlan 2

SW-1(config-if)# end

SW-1# show running-config

3. ¿Cuántas interfaces FastEthernet están asignadas a la V-LAN 1?

Seis, desde la FastEthernet 0/1 hasta la FastEthernet 0/6

4. ¿ Cuántas interfaces FastEthernet están asignadas a la V-LAN 2?

Seis, desde la FastEthernet 0/7 hasta la FastEthernet 0/12

Paso 3 - Probar la funcionalidad de las 2 VLAN utilice el comando ping en cada estación de trabajo y contestar las siguientes preguntas:

5. Emita un ping del PC1 a las demás estaciones de trabajo. ¿El ping fue exitoso?

El ping fue exitoso en la estación de trabajo PC2 porque pertenece a la misma V-LAN 1, y no tuvo éxito en las estaciones de trabajo PC3 y PC4 porque pertenecen a otra V-LAN (V-LAN 2).

6. Cambie el PC1 del puerto 1 al puerto 7 y emita un ping a las demás estaciones. ¿qué ocurrió?

El ping fue exitoso en las estaciones de trabajo PC3 y PC4 porque pertenecen a la misma V-LAN 2, y no tuvo éxito en la estación de trabajo PC1 porque pertenece a otra V-LAN (V-LAN 1).

4.2 PRÁCTICA DE V-LAN POR PUERTO CON DOS SWITCH

Duración estimada: 60 min.

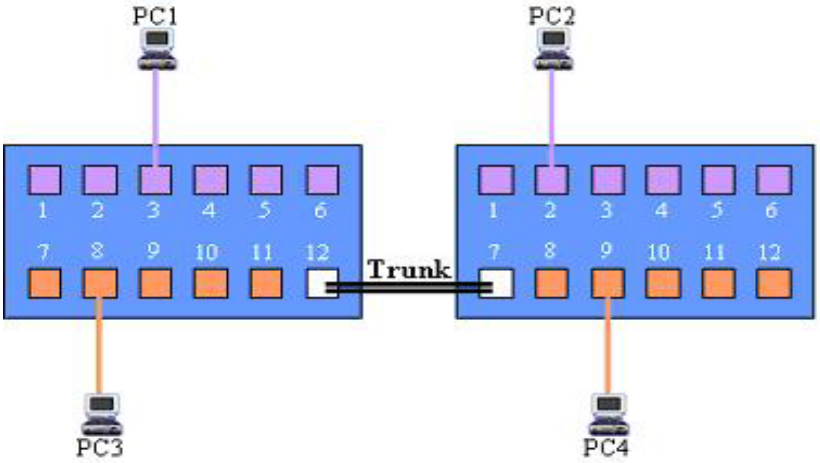


Figura 4.2 V-LAN con dos Switch

Nombre del Switch 1 : SW-1	Nombre del Switch 2 : SW-2
Tipo de Switch : 2950	Tipo de Switch : 2950
Nombre de V-LAN1 : alumnos	Nombre de V-LAN1 : alumnos
Nombre de V-LAN2 : profesores	Nombre de V-LAN2 : profesores
Puertos para V-LAN1 : 1,2,3,4,5 y 6	Puertos para V-LAN1 : 1,2,3,4,5 y 6
Puertos para V-LAN2 : 7,8,9,10 y11	Puertos para V-LAN2 : 8,9,10,11 y12
Puerto de Trunk : 12	Puerto de Trunk : 7
IP de los PCs de la V-LAN1 : 172.20.40.(3-8) 255.255.252.0 Puerta de enlace : 172.20.40.1	IP de los PCs de la V-LAN1 : 172.20.40.(9-14) 255.255.252.0 Puerta de enlace : 172.20.40.1
IP de los PCs de la V-LAN2 : 172.20.44.(3-7) 255.255.252.0 Puerta de enlace : 172.20.44.1	IP de los PCs de la V-LAN2 : 172.20.44.(9-13) 255.255.252.0 Puerta de enlace : 172.20.44.1

LEYENDA

 = Switch

 = usuarios

= V-LAN1 (alumnos)

= V-LAN2 (profesores)

= Trunk

4.2.1 Objetivos

Esta práctica de laboratorio sirve para practicar las siguientes tareas:

- Conectarse a través de la consola a dos Switch para crear o configurar 2 V-LANs en cada Switch con sus respectivos nombres
- Probar o hacer ping entre cada uno de los Host conectados a cada V-LAN en cada Switch
- Conectar y configurar el enlace Trunk entre dos Switch
- Probar o hacer ping entre cada uno de los Host conectados a cada V-LAN entre cada Switch por medio del Trunking

4.2.2 Información básica

En esta práctica de laboratorio se trabaja con redes de área local virtuales Ethernet (V-LAN). Normalmente todos los puertos en un Switch están en la misma VLAN 1 por defecto. En esta práctica implementaremos las V-LANs (VLAN 1 y VLAN 2) por puerto en dos Switch, donde cada puerto en cada Switch puede asociarse a una VLAN. Para compartir V-LANs entre Switches debe establecerse una conexión entre estos por medio del comando trunk configurado en un puerto especifico en cada Switch. Si un Switch con 12 puertos se divide en 2 VLAN de 6 puertos cada uno, los usuarios de una VLAN no podrán acceder a los recursos (como servidores o impresoras) en la otra VLAN.

Accederá mediante la consola al Switch para configurar las VLAN. Esta práctica de laboratorio ayudará a demostrar cómo varias V-LANs en Switches diferentes, se pueden comunicar usando Trunking.

4.2.3 Herramientas / preparación

Antes de comenzar con la práctica de laboratorio, el profesor o asistente de laboratorio debe preparar dos Switch con los valores VLAN por defecto. Se debe colocar también a disposición dos estaciones de trabajo con HyperTerminal para realizar la conexión de consola al Switch. A continuación se suministra la lista de equipo requerido.

- Dos estaciones de PC con HyperTerminal instalado para configurar cada Switch
- Cuatro estaciones de PC Windows
- 2 Switch Cisco (modelo 2900 Series)
- 2 cables de consola (roll-over) y dos adaptadores DB-9/RJ45 o cables de módem nulo DB-9
- Cable Ethernet CAT 6 desde cada estación de trabajo a un puerto Ethernet de cada Switch

4.2.4 Recursos Web

- LAN Switching basics www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/lanswtch.htm
- General information on all Cisco products - (Ir al capítulo 22 - Switches) www.cisco.com/univercd/cc/td/doc/pcat/#2
- 1900 / 2820 series Ethernet switches www.cisco.com/warp/public/cc/pd/si/casi/ca1900/prodlit/s1928_ov.htm
- 2900 series Fast Ethernet switches www.cisco.com/warp/public/cc/pd/si/casi/ca2900xl/prodlit/s290xl_ov.htm
- 3500 series Gigabit Ethernet switches www.cisco.com/warp/public/cc/pd/si/casi/ca3500/prodlit/s3500x_ov.htm

- Virtual LAN for 1900/2820 Switches

  www.cisco.com/univercd/cc/td/doc/product/lan/28201900/1928v8x/eesc98x/02vlans.htm

4.2.5 Notas

4.2.6 Comandos a utilizar en la práctica de V-LAN por puerto con dos Switch

Comandos	Descripción
configure terminal	Entra al modo de configuración global. Realiza la configuración desde la terminal de consola de forma manual
End	Sale del modo de configuración
interface fastEthernet 0/id	Entra a una de las interfaces FastEthernet establecidas por el usuario
Ping	Utiliza el protocolo ICMP para verificar la conexión de hardware y la dirección lógica en la capa de internet, envía mensajes de eco al dispositivo vecino
show running-config	Muestra el archivo de configuración activo o muestra la configuración actual en la RAM
show vlan	Muestra todas la V-LANs con sus respectivos puertos asignados a cada una de ellas
switchport mode access vlan id	Asigna un puerto o un rango de

	puertos a una V-LAN
vlan database	Entra al modo de configuración de las VLAN
vlan vlan-id **name** vlan-name	Crea una V-LAN con un número (1-1001) determinado y a la vez le coloca un nombre
switchport mode trunk	Define un puerto como trunk
switchport trunk allowed vlan all	Determina que todas las V-LAN del Switch tendrán acceso al puerto trunk

Tabla 4.2 Comandos de la práctica de V-LAN con dos Switch

4.2.7 Pasos para la práctica de V-LAN por puerto con dos Switch

Seleccione dos Switch (modelo Cisco 2950 Series) y 4 PCs antes de comenzar la práctica de Laboratorio. Conecte una estación de trabajo a la conexión del puerto de consola de cada Switch para configurar cada puerto con su respectiva V-LAN, conecte los 2 computadores al Switch 1 en los puertos 3 y 8, y conecte los 2 computadores al Switch 2 en los puertos 2 y 9.

Paso 1 – Utilizar el diagrama de laboratorio, colocar los siguientes comandos para crear V-LANs con el Switch 1 y responda las siguientes preguntas:

SW-1# vlan database

SW-1(vlan)# vlan 2 name profesores

SW-1# show vlan

1. ¿Cuántos puertos están asignados a la V-LAN 1?

_____

2. ¿Cuántos puertos están asignados a la V-LAN 2?

_____

Paso 2 – Asignar puertos a cada V-LAN en el Switch 1 con los siguientes comandos y contestar las siguientes preguntas:

SW-1# configure terminal

SW-1(config)# interface fastEthernet 0/7

SW-1(config-if)# switchport mode access vlan 2

SW-1(config-if)# end

SW-1# configure terminal

SW-1(config)# interface fastEthernet 0/8

SW-1(config-if)# switchport mode access vlan 2

SW-1(config-if)# end

SW-1# configure terminal

SW-1(config)# interface fastEthernet 0/9

SW-1(config-if)# switchport mode access vlan 2

SW-1(config-if)# end

SW-1# configure terminal

SW-1(config)# interface fastEthernet 0/10

SW-1(config-if)# switchport mode access vlan 2

SW-1(config-if)# end

SW-1# configure terminal

SW-1(config)# interface fastEthernet 0/11

SW-1(config-if)# switchport mode access vlan 2

SW-1(config-if)# end

SW-1# show running-config

3. ¿Cuántas interfaces FastEthernet están asignadas a la V-LAN 1?

_____

4. ¿ Cuántas interfaces FastEthernet están asignadas a la V-LAN 2?

_____

Paso 3 - Probar la funcionalidad de las 2 VLAN en el Switch 1, utilice el comando ping en cada estación de trabajo y contestar las siguientes preguntas:

5. Emita un ping del PC1 a las demás estaciones de trabajo. ¿El ping fue exitoso?

_____

6. Cambie el PC1 del puerto 1 al puerto 7 y emita un ping a la estación PC3. ¿qué ocurrió?

_____

Cambie el PC1 al puerto 1 para seguir con el diagrama inicial.

Paso 4 – Configuración del puerto Trunk en el puerto 12 del Switch 1 con los siguientes comandos y contestar las siguientes preguntas:

SW-1# configure terminal

SW-1(config)# interface fastEthernet 0/12

SW-1(config-if)# switchport mode trunk

SW-1 (config-if)# switchport trunk allowed vlan all

SW-1 (config-if)# end

SW-1# show interfaces fastEthernet 0/12

7. ¿Como esta el modo administrativo de la interfaz del puerto 12?

_____

8. ¿Cuántas V-LANs tienen acceso al puerto Trunk?

_____

Paso 5 – Utilizar el diagrama de laboratorio, colocar los siguientes comandos para crear V-LANs con el Switch 2 y responda las siguientes preguntas:

SW-2# vlan database

SW-2(vlan)# vlan 2 name profesores

SW-2# show vlan

9. ¿Cuántos puertos están asignados a la V-LAN 1?

_____

10. ¿Cuántos puertos están asignados a la V-LAN 2?

_____

Paso 6 – Asignar puertos a cada V-LAN en el Switch 2 con los siguientes comandos y contestar las siguientes preguntas:

SW-2# configure terminal

SW-2(config)# interface fastEthernet 0/8

SW-2(config-if)# switchport mode access vlan 2

SW-2(config-if)# end

SW-2# configure terminal

SW-2(config)# interface fastEthernet 0/9

SW-2(config-if)# switchport mode access vlan 2

SW-2(config-if)# end

SW-2# configure terminal

SW-2(config)# interface fastEthernet 0/10

SW-2(config-if)# switchport mode access vlan 2

SW-2(config-if)# end

SW-2# configure terminal

SW-2(config)# interface fastEthernet 0/11

SW-2(config-if)# switchport mode access vlan 2

SW-2(config-if)# end

SW-2# configure terminal

SW-2(config)# interface fastEthernet 0/12

SW-2(config-if)# switchport mode access vlan 2

SW-2(config-if)# end

SW-2# show running-config

11. ¿Cuántas interfaces FastEthernet están asignadas a la V-LAN 1?

_____

12. ¿ Cuántas interfaces FastEthernet están asignadas a la V-LAN 2?

_____

Paso 7 - Probar la funcionalidad de las 2 VLAN en el Switch 2, utilice el comando ping en cada estación de trabajo y contestar las siguientes preguntas:

13. Emita un ping del PC2 a las demás estaciones de trabajo. ¿El ping fue exitoso?

_____

14. Cambie el PC2 del puerto 1 al puerto 8 y emita un ping a la estación PC4. ¿qué ocurrió?

_____

Cambie el PC2 al puerto 2 para seguir con el diagrama inicial.

Paso 8 – Configuración del puerto Trunk en el puerto 7 del Switch 2 con los siguientes comandos y contestar las siguientes preguntas:

SW-2# configure terminal

SW-2(config)# interface fastEthernet 0/7

SW-2(config-if)# switchport mode trunk

SW-2 (config-if)# switchport trunk allowed vlan all

SW-2 (config-if)# end

SW-2# show interfaces fastEthernet 0/7

15. ¿Como esta el modo administrativo de la interfaz del puerto 7?

_____

16. ¿Cuántas V-LANs tienen acceso al puerto Trunk?

_____

Paso 9 – Comprobar la comunicación entre la V-LAN 1 del Switch 1 y la V-LAN 1 del Switch 2 por Trunking y la comunicación entre la V-LAN 2 del Switch 1 y la V-LAN 2 del Switch 2 por Trunking. Para

esto, utilizar el comando ping entre las PCs y contestar las siguientes preguntas:

17. Emita un ping del PC1 al PC2 y al PC4. ¿El ping fue exitoso?

_____

_____

18. Emita un ping del PC4 al PC1 y al PC3. ¿El ping fue exitoso?

_____

_____

4.2.8 Respuestas de la práctica de V-LAN por puerto con dos Switch

Paso 1 – Utilizar el diagrama de laboratorio, colocar los siguientes comandos para crear V-LANs con el Switch 1 y responda las siguientes preguntas:

SW-1# vlan database

SW-1(vlan)# vlan 2 name profesores

SW-1# show vlan

1. ¿Cuántos puertos están asignados a la V-LAN 1?

Todos los puertos pertenecen a la V-LAN 1 (alumnos)

2. ¿Cuántos puertos están asignados a la V-LAN 2?

Ninguno, porque no se ha configurado los puertos del Switch para la VLAN 2, sólo se le coloco el nombre profesores a una posible V-LAN 2.

Paso 2 – Asignar puertos a cada V-LAN en el Switch 1 con los siguientes comandos y contestar las siguientes preguntas:

SW-1# configure terminal

SW-1(config)# interface fastEthernet 0/7

SW-1(config-if)# switchport mode access vlan 2

SW-1(config-if)# end

SW-1# configure terminal

SW-1(config)# interface fastEthernet 0/8

SW-1(config-if)# switchport mode access vlan 2

SW-1(config-if)# end

SW-1# configure terminal

SW-1(config)# interface fastEthernet 0/9

SW-1(config-if)# switchport mode access vlan 2

SW-1(config-if)# end

SW-1# configure terminal

SW-1(config)# interface fastEthernet 0/10

SW-1(config-if)# switchport mode access vlan 2

SW-1(config-if)# end

SW-1# configure terminal

SW-1(config)# interface fastEthernet 0/11

SW-1(config-if)# switchport mode access vlan 2

SW-1(config-if)# end

SW-1# show running-config

3. ¿Cuántas interfaces FastEthernet están asignadas a la V-LAN 1?

Seis, desde la FastEthernet 0/1 hasta la FastEthernet 0/6

4. ¿ Cuántas interfaces FastEthernet están asignadas a la V-LAN 2?

Seis, desde la FastEthernet 0/7 hasta la FastEthernet 0/11

Paso 3 - Probar la funcionalidad de las 2 VLAN en el Switch 1, utilice el comando ping en cada estación de trabajo y contestar las siguientes preguntas:

5. Emita un ping del PC1 a las demás estaciones de trabajo. ¿El ping fue exitoso?

El ping no fue exitoso en la estación de trabajo PC3 porque no pertenece a la misma V-LAN.

6. Cambie el PC1 del puerto 1 al puerto 7 y emita un ping a la estación PC3. ¿qué ocurrió?

El ping fue exitoso en la estación de trabajo PC3 porque pertenecen a la misma V-LAN.

Cambie el PC1 al puerto 1 para seguir con el diagrama inicial.

Paso 4 – Configuración del puerto Trunk en el puerto 12 del Switch 1 con los siguientes comandos y contestar las siguientes preguntas:

SW-1# configure terminal

SW-1(config)# interface fastEthernet 0/12

SW-1(config-if)# switchport mode trunk

SW-1 (config-if)# switchport trunk allowed vlan all

SW-1 (config-if)# end

SW-1# show interfaces fastEthernet 0/12

7. ¿Como esta el modo administrativo de la interfaz del puerto 12?

Esta configurado como Trunk

8. ¿Cuántas V-LANs tienen acceso al puerto Trunk?

Todas las V-LANs

Paso 5 – Utilizar el diagrama de laboratorio, colocar los siguientes comandos para crear V-LANs con el Switch 2 y responda las siguientes preguntas:

SW-2# vlan database

SW-2(vlan)# vlan 2 name profesores

SW-2# show vlan

9. ¿Cuántos puertos están asignados a la V-LAN 1?

Todos los puertos pertenecen a la V-LAN 1 (alumnos)

10. ¿Cuántos puertos están asignados a la V-LAN 2?

Ninguno, porque no se ha configurado los puertos del Switch para la VLAN 2, sólo se le coloco el nombre profesores a una posible V-LAN 2.

Paso 6 – Asignar puertos a cada V-LAN en el Switch 2 con los siguientes comandos y contestar las siguientes preguntas:

SW-2# configure terminal

SW-2(config)# interface fastEthernet 0/8

SW-2(config-if)# switchport mode access vlan 2

SW-2(config-if)# end

SW-2# configure terminal

SW-2(config)# interface fastEthernet 0/9

SW-2(config-if)# switchport mode access vlan 2

SW-2(config-if)# end

SW-2# configure terminal

SW-2(config)# interface fastEthernet 0/10

SW-2(config-if)# switchport mode access vlan 2

SW-2(config-if)# end

SW-2# configure terminal

SW-2(config)# interface fastEthernet 0/11

SW-2(config-if)# switchport mode access vlan 2

SW-2(config-if)# end

SW-2# configure terminal

SW-2(config)# interface fastEthernet 0/12

SW-2(config-if)# switchport mode access vlan 2

SW-2(config-if)# end

SW-2# show running-config

11. ¿Cuántas interfaces FastEthernet están asignadas a la V-LAN 1?

Seis, desde la FastEthernet 0/1 hasta la FastEthernet 0/6

12. ¿ Cuántas interfaces FastEthernet están asignadas a la V-LAN 2?

Seis, desde la FastEthernet 0/8 hasta la FastEthernet 0/12

Paso 7 - Probar la funcionalidad de las 2 VLAN en el Switch 2, utilice el comando ping en cada estación de trabajo y contestar las siguientes preguntas:

13. Emita un ping del PC2 a las demás estaciones de trabajo. ¿El ping fue exitoso?

El ping no fue exitoso en la estación de trabajo PC4 porque no pertenece a la misma V-LAN.

14. Cambie el PC2 del puerto 1 al puerto 8 y emita un ping a la estación PC4. ¿qué ocurrió?

El ping fue exitoso en la estación de trabajo PC4 porque pertenecen a la misma V-LAN.

Cambie el PC2 al puerto 2 para seguir con el diagrama inicial.

Paso 8 – Configuración del puerto Trunk en el puerto 7 del Switch 2 con los siguientes comandos y contestar las siguientes preguntas:

SW-2# configure terminal

SW-2(config)# interface fastEthernet 0/7

SW-2(config-if)# switchport mode trunk

SW-2 (config-if)# switchport trunk allowed vlan all

SW-2 (config-if)# end

SW-2# show interfaces fastEthernet 0/7

15. ¿Como esta el modo administrativo de la interfaz del puerto 7?

Esta configurado como Trunk

16. ¿Cuántas V-LANs tienen acceso al puerto Trunk?

Todas las V-LANs

Paso 9 – Comprobar la comunicación entre la V-LAN 1 del Switch 1 y la V-LAN 1 del Switch 2 por Trunking y la comunicación entre la V-LAN 2 del Switch 1 y la V-LAN 2 del Switch 2 por Trunking. Para esto, utilizar el comando ping entre las PCs y contestar las siguientes preguntas:

17. Emita un ping del PC1 al PC2 y al PC4. ¿El ping fue exitoso?

El ping no fue exitoso en la estación de trabajo PC4 porque pertenece a la V-LAN 2 y fue exitoso en el PC2 porque pertenece a la V-LAN 1

18. Emita un ping del PC4 al PC1 y al PC3. ¿El ping fue exitoso?

El ping no fue exitoso en la estación de trabajo PC1 porque pertenece a la V-LAN 1 y fue exitoso en el PC3 porque pertenece a la V-LAN 2

4.3 PRÁCTICA DE COMUNICACIÓN ENTRE V-LAN CON UN SWITCH POR MEDIO DE UN ROUTER

Duración estimada: 60 min.

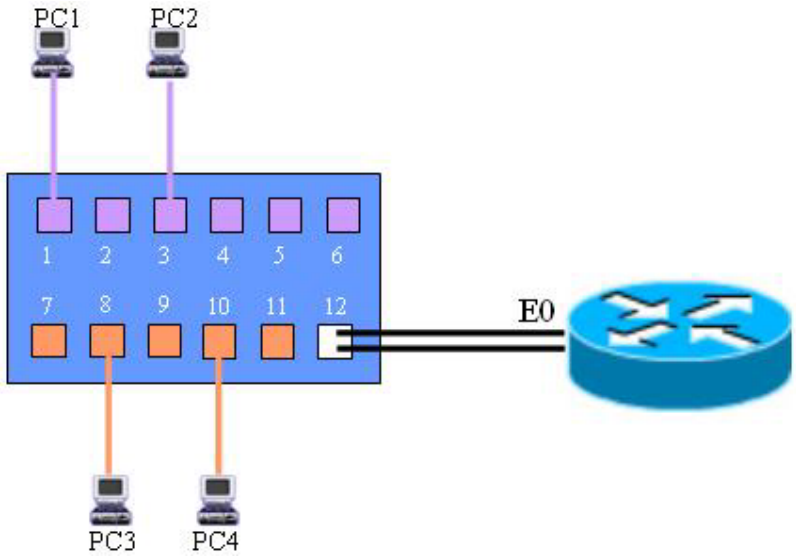


Figura 4.3 V-LAN con un Switch y un Router

Nombre del Switch 1 : SW-1
Tipo de Switch : 2950
Nombre de V-LAN1 : alumnos
Nombre de V-LAN2 : profesores
Puertos para V-LAN1 : 1,2,3,4,5 y 6
Puertos para V-LAN2 : 7,8,9,10 y11
Puerto de Trunk : 12
IP de los PCs de la V-LAN1 : 172.20.40.(3-8) 255.255.252.0 Puerta de enlace : 172.20.40.1
IP de los PCs de la V-LAN2 : 172.20.44.(3-7) 255.255.252.0 Puerta de enlace : 172.20.44.1

Nombre del Router : LAB-A
Tipo de Router : 2620
E0/0.1 : 172.20.40.1 255.255.252.0
E0/0.2 : 172.20.44.1 255.255.252.0

LEYENDA

 = Router

 = Switch

 = usuarios

= V-LAN1 (alumnos)

= V-LAN2 (profesores)

= Trunk

4.3.1 Objetivos

Esta práctica de laboratorio sirve para practicar las siguientes tareas:

- Conectar a través de la consola al Switch para crear y configurar 2 VLANs en el Switch con sus respectivos nombres
- Probar o hacer ping entre cada uno de los Host conectados a cada V-LAN del Switch para verificar la comunicación entre los PCs
- Configurar el enlace Trunk en el Switch para comunicarse con el Router
- Configurar la fastethernet del Router para dar soporte a VLANs permitiendo así la intercomunicación entre ellas
- Probar o hacer ping entre cada uno de los Host conectados a cada V-LAN del Switch para verificar la intercomunicación entre las V-LAN por capa 3

4.3.2 Información básica

Para limitar los dominios de difusión a nivel de LAN se ha creado el concepto de VLAN. La implementación de las VLANs se realiza a nivel de capa 2, por lo que pueden ser implementadas en un Switch. El objetivo es que los dominios de difusión no se asignen por la pertenencia a una determinada red LAN, sino que éstos son definidos en función del puerto del Switch. La implementación de una VLAN se realiza asignado cada puerto del Switch a una determinada VLAN, limitando la difusión de mensajes entre los dispositivos (puertos) que pertenecen a la misma VLAN. Las VLAN se pueden propagar a través de una jerarquía de Switch pero no pueden propagarse más allá de un Router, ya que el Router separa por sí mismo dominios de difusión, por lo que no tiene sentido el que las VLAN se propaguen a través de él.

Cuando configuramos un Switch (o grupo de Switches) para que soporte distintas VLANs, es como si en realidad nuestro Switch (o grupo de Switches) lo estuviéramos dividiendo en varias LANs distintas una por cada VLAN. De ahí que necesitemos de un Router para poder intercomunicarlas entre ellas, la comunicación entre dispositivos de una misma VLAN (LAN) se realiza a nivel de capa 2 (direcciones MAC), pero la comunicación entre dispositivos de distintas VLANs (LANs) se realiza a nivel de capa 3 (direcciones IP). Consecuencia de esto es que a cada VLAN se le debe de asignar un espacio de direcciones distinto, debiéndose de realizar subneting en la subred.

4.3.3 Herramientas / preparación

Antes de comenzar con la práctica de laboratorio, el profesor o asistente de laboratorio debe preparar un Switch con los valores VLAN por defecto, un Router, dos estaciones de trabajo con HyperTerminal para realizar la conexión de consola al Switch y al Router. A continuación se suministra la lista de equipo requerido.

- Dos estaciones de PC con HyperTerminal instalado para configurar el Switch y el Router
- Cuatro estaciones de PC Windows
- Un Switch Cisco (modelo 2900 Series)
- Un Router Cisco (modelo 2600 Series)
- 2 cables de consola (roll-over) y dos adaptadores DB-9/RJ45 o cables de módem nulo DB-9
- Cable Ethernet CAT 6 desde cada estación de trabajo a un puerto Ethernet de cada Switch

4.3.6 Recursos Web

- LAN Switching basics www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/lanswtch.htm
- General information on all Cisco products - (Ir al capítulo 22 - Switches) www.cisco.com/univercd/cc/td/doc/pcat/#2

- 1900 / 2820 series Ethernet switches
  www.cisco.com/warp/public/cc/pd/si/casi/ca1900/prodlit/s1928_ov.htm
- 2900 series Fast Ethernet switches
  cisco.com/warp/public/cc/pd/si/casi/ca2900xl/prodlit/s290xl_ov.htm
- 3500 series Gigabit Ethernet switches
  cisco.com/warp/public/cc/pd/si/casi/ca3500/prodlit/s3500x_ov.htm
- Virtual LAN for 1900/2820 Switches
  www.cisco.com/univercd/cc/td/doc/product/lan/28201900/1928v8x/eesc98x/02vlans.htm
- Información general acerca de los routers
  www.cisco.com/univercd/cc/td/doc/pcat/#2
- Routers de la Serie 2500
  www.cisco.com/warp/public/cc/cisco/mkt/access/2500/index.shtml

4.3.5 Notas

4.3.6 Comandos a utilizar en la práctica de comunicación entre VLAN con un Switch por medio de un Router

- **Comandos en el Switch**

Comandos	Descripción
configure terminal	Entra al modo de configuración global. Realiza la configuración desde la terminal de consola de forma manual
End	Sale del modo de configuración
interface fastEthernet 0/id	Entra a una interface FastEthernet establecidas por el usuario
interface vlan id	Entra a la interface de una V-LAN
Ip address	Coloca una dirección ip
Ip default-gateway ip	Coloca una dirección de puerta de enlace
Ping	Utiliza el protocolo ICMP para verificar la conexión de hardware y la dirección lógica en la capa de internet, envía mensajes de eco al dispositivo vecino
show running-config	Muestra el archivo de configuración activo o muestra la configuración

	actual en la RAM
show vlan	Muestra todas la V-LANs con sus respectivos puertos asignados a cada una de ellas
switchport mode access vlan id	Asigna un puerto o un rango de puertos a una V-LAN
switchport mode trunk	Define un puerto como trunk
switchport trunk allowed vlan all	Determina que todas las V-LAN del Switch tendrán acceso al puerto trunk
vlan database	Entra al modo de configuración de las VLAN
vlan vlan-id **name** vlan-name	Crea una V-LAN con un número (1-1001) determinado y a la vez le coloca un nombre

Tabla 4.3 Comandos del Switch para la práctica de V-LAN con un Router

- **Comandos en el Router**

Comandos	Descripción
Configure terminal	Realiza la configuración desde la terminal de consola de forma manual
Encapsulation dot1Q 2	Especifica que una interface utiliza un etiquetado de V-LANS basado en el estándar IEEE 802.1Q
interface fastEthernet	Entra a la configuración de la interfaz Ethernet
ip address	Coloca una dirección ip
No shutdown	Habilita la interfaz deseada
Ping	Utiliza el protocolo ICMP para verificar la conexión de hardware y la dirección lógica en la capa de internet, envía mensajes de eco al dispositivo vecino
show interface serial	Muestra estadísticas de la interface serial configurada en el Router
show running-config	Muestra el archivo de configuración activo o muestra la configuración actual en la RAM

Tabla 4.4 Comandos del Router para la práctica de V-LAN con un Router

4.3.7 Pasos para la práctica de práctica de comunicación entre VLAN con un Switch por medio de un Router

Seleccione un Switch (modelo Cisco 2950 Series), un Router (Modelo 2600 series) y 4 PCs antes de comenzar la práctica de laboratorio. Conectar una estación de trabajo a la conexión del puerto de consola del Switch para configurar cada puerto con su respectiva V-LAN (V-LAN1 y V-LAN2), conectar los 4 computadores al Switch en los puertos 1, 3, 8 y 10, conectar el puerto 12 del Switch con la interfaz FastEthernet 0/0 del Router.

Paso 1 – Utilizar el diagrama de laboratorio, colocar los siguientes comandos para crear V-LANs en el Switch y responda las siguientes preguntas:

SW-1# vlan database

SW-1(vlan)# vlan 2 name profesores

SW-1# show vlan

1. ¿Cuántos puertos están asignados a la V-LAN 1?

_____

2. ¿Cuántos puertos están asignados a la V-LAN 2?

_____

Paso 2 – Configurar la IP y la puerta de enlace para cada V-LAN en el Switch, para acceder de manera remota al Router, para esto, utilizar los siguientes comandos y contestar las siguientes preguntas:

SW-1# configure terminal

SW-1(config)# interface vlan 1

SW-1(config-if)# ip address 172.20.40.2 255.255.252.0

SW-1(config-if)# exit

SW-1(config)# interface vlan 1

SW-1(config-if)# ip default-gateway 172.20.40.1

SW-1(config-if)# no shutdown

SW-1(config-if)# end

SW-1# configure terminal

SW-1(config)# interface vlan 2

SW-1(config-if)# ip address 172.20.44.2 255.255.252.0

SW-1(config-if)# exit

SW-1(config)# interface vlan 2

SW-1(config-if)# ip default-gateway 172.20.44.1

SW-1(config-if)# no shutdown

SW-1(config-if)# end

SW-1# show running-config

3. ¿Muestra la IP de la V-LAN 1 y la IP de la V-LAN 2?

4. ¿Muestra la puerta de enlace de la V-LAN 1 y la V-LAN 2?

Paso 3 – Asignar puertos a cada V-LAN en el Switch con los siguientes comandos y contestar las siguientes preguntas:

SW-1# configure terminal

SW-1(config)# interface fastEthernet 0/7

SW-1(config-if)# switchport mode access vlan 2

SW-1(config-if)# end

SW-1# configure terminal

SW-1(config)# interface fastEthernet 0/8

SW-1(config-if)# switchport mode access vlan 2

SW-1(config-if)# end

SW-1# configure terminal

SW-1(config)# interface fastEthernet 0/9

SW-1(config-if)# switchport mode access vlan 2

SW-1(config-if)# end

SW-1# configure terminal

SW-1(config)# interface fastEthernet 0/10

SW-1(config-if)# switchport mode access vlan 2

SW-1(config-if)# end

SW-1# configure terminal

SW-1(config)# interface fastEthernet 0/11

SW-1(config-if)# switchport mode access vlan 2

SW-1(config-if)# end

SW-1# show running-config

5. ¿Cuántas interfaces FastEthernet están asignadas a la V-LAN 1?

_____

6. ¿ Cuántas interfaces FastEthernet están asignadas a la V-LAN 2?

_____

Paso 4 - Probar la funcionalidad de las 2 VLAN en el Switch, utilizar el comando ping en cada estación de trabajo y contestar las siguientes preguntas:

7. Emita un ping del PC1 a las demás estaciones de trabajo. ¿El ping fue exitoso? 0

_____

_____

8. Cambie el PC1 del puerto 1 al puerto 7 y emita un ping a la estación PC3. ¿qué ocurrió?

_____

Cambie el PC1 al puerto 1 para seguir con el diagrama inicial.

Paso 5 – Configuración del puerto Trunk en el puerto 12 del Switch con los siguientes comandos y contestar las siguientes preguntas:

SW-1# configure terminal

SW-1(config)# interface fastEthernet 0/12

SW-1(config-if)# switchport mode trunk

SW-1 (config-if)# switchport trunk allowed vlan all

SW-1 (config-if)# end

SW-1# show interfaces fastEthernet 0/12

9. ¿Como esta el modo administrativo de la interfaz del puerto 12?

_____

10. ¿Cuántas V-LANs tienen acceso al puerto Trunk?

_____

Paso 6 – Configurar la comunicación de V-LAN en el Router con los siguientes comandos y contestar las siguientes preguntas:

LAB-A# configure terminal

LAB-A(config)# interface fastEthernet 0/0

LAB-A(config-if)# ip address 172.20.40.1 255.255.252.0

LAB-A(config-if)# no shutdown

LAB-A(config-if)# end

LAB-A# configure terminal

LAB-A (config)#interface fastEthernet 0/0.2

LAB-A (config-subif)#encapsulation dot1Q 2

LAB-A (config-subif)#ip address 172.20.44.1 255.255.252.0

LAB-A (config-subif)#exit

LAB-A# show running-configure

11. ¿ Muestra la IP de la interface fastEthernet 0/0 y la IP interface fastEthernet 0/0.2?

_____

_____

Paso 7 – Comprobar la comunicación entre las V-LANs del Switch por medio del Router. Para esto, utilizar el comando ping entre las PCs y contestar las siguientes preguntas:

17. Emita un ping del PC1 a todas las estaciones. ¿El ping fue exitoso?

_____

_____

4.3.8 Respuestas de la práctica de comunicación entre V-LAN con un Switch por medio de un Router

Paso 1 – Utilizar el diagrama de laboratorio, colocar los siguientes comandos para crear V-LANs en el Switch y responda las siguientes preguntas:

SW-1# vlan database

SW-1(vlan)# vlan 2 name profesores

SW-1# show vlan

1. ¿Cuántos puertos están asignados a la V-LAN 1?

Todos los puertos pertenecen a la V-LAN 1 (alumnos)

2. ¿Cuántos puertos están asignados a la V-LAN 2?

Ninguno, porque no se ha configurado los puertos del Switch para la VLAN 2, sólo se le coloco el nombre profesores a una posible V-LAN 2.

Paso 2 – Configurar la IP y la puerta de enlace para cada V-LAN en el Switch, para acceder de manera remota al Router, para esto, utilizar los siguientes comandos y contestar las siguientes preguntas:

SW-1# configure terminal

SW-1(config)# interface vlan 1

SW-1(config-if)# ip address 172.20.40.2 255.255.252.0

SW-1(config-if)# exit

SW-1(config)# interface vlan 1

SW-1(config-if)# ip default-gateway 172.20.40.1

SW-1(config-if)# no shutdown

SW-1(config-if)# end

SW-1# configure terminal

SW-1(config)# interface vlan 2

SW-1(config-if)# ip address 172.20.44.2 255.255.252.0

SW-1(config-if)# exit

SW-1(config)# interface vlan 2

SW-1(config-if)# ip default-gateway 172.20.44.1

SW-1(config-if)# no shutdown

SW-1(config-if)# end

SW-1# show running-config

3. ¿Muestra la IP de la V-LAN 1 y la IP de la V-LAN 2?

Si, IP de la V-LAN 1 es 172.20.40.2 y la IP de la V-LAN 2 es 172.20.44.2

4. ¿Muestra la puerta de enlace de la V-LAN 1 y la V-LAN 2?

Si, la puerta de enlace de la V-LAN 1 es 172.20.40.1 y de la V-LAN 2 es 172.20.44.1

Paso 3 – Asignar puertos a cada V-LAN en el Switch con los siguientes comandos y contestar las siguientes preguntas:

SW-1# configure terminal

SW-1(config)# interface fastEthernet 0/7

SW-1(config-if)# switchport mode access vlan 2

SW-1(config-if)# end

SW-1# configure terminal

SW-1(config)# interface fastEthernet 0/8

SW-1(config-if)# switchport mode access vlan 2

SW-1(config-if)# end

SW-1# configure terminal

SW-1(config)# interface fastEthernet 0/9

SW-1(config-if)# switchport mode access vlan 2

SW-1(config-if)# end

SW-1# configure terminal

SW-1(config)# interface fastEthernet 0/10

SW-1(config-if)# switchport mode access vlan 2

SW-1(config-if)# end

SW-1# configure terminal

SW-1(config)# interface fastEthernet 0/11

SW-1(config-if)# switchport mode access vlan 2

SW-1(config-if)# end

SW-1# show running-config

5. ¿Cuántas interfaces FastEthernet están asignadas a la V-LAN 1?

Seis, desde la FastEthernet 0/1 hasta la FastEthernet 0/6

6. ¿ Cuántas interfaces FastEthernet están asignadas a la V-LAN 2?

Seis, desde la FastEthernet 0/7 hasta la FastEthernet 0/11

Paso 4 - Probar la funcionalidad de las 2 VLAN en el Switch, utilizar el comando ping en cada estación de trabajo y contestar las siguientes preguntas:

7. Emita un ping del PC1 a las demás estaciones de trabajo. ¿El ping fue exitoso?

El ping no fue exitoso en las estaciones de trabajo PC3 y PC4 porque pertenecen a la V-LAN 2 y fue exitoso en la estación de trabajo PC2 porque pertenece a la V-LAN 1

8. Cambie el PC1 del puerto 1 al puerto 7 y emita un ping a la estación PC3. ¿qué ocurrió?

El ping fue exitoso en las estaciones de trabajo PC3 y PC4 porque pertenecen a la V-LAN 2 y no fue exitoso en la estación de trabajo PC2 porque pertenece a la V-LAN 1

Cambie el PC1 al puerto 1 para seguir con el diagrama inicial.

Paso 5 – Configuración del puerto Trunk en el puerto 12 del Switch con los siguientes comandos y contestar las siguientes preguntas:

SW-1# configure terminal

SW-1(config)# interface fastEthernet 0/12

SW-1(config-if)# switchport mode trunk

SW-1 (config-if)# switchport trunk allowed vlan all

SW-1 (config-if)# end

SW-1# show interfaces fastEthernet 0/12

9. ¿Como esta el modo administrativo de la interfaz del puerto 12?

Esta configurado como Trunk

10. ¿Cuántas V-LANs tienen acceso al puerto Trunk?

Todas las V-LANs

Paso 6 – Configurar la comunicación de V-LAN en el Router con los siguientes comandos y contestar las siguientes preguntas:

LAB-A# configure terminal

LAB-A(config)# interface fastEthernet 0/0

LAB-A(config-if)# ip address 172.20.40.1 255.255.252.0

LAB-A(config-if)# no shutdown

LAB-A(config-if)# end

LAB-A# configure terminal

LAB-A (config)#interface fastEthernet 0/0.2

LAB-A (config-subif)#encapsulation dot1Q 2

LAB-A (config-subif)#ip address 172.20.44.1 255.255.252.0

LAB-A (config-subif)#exit

LAB-A# show running-configure

11. ¿ Muestra la IP de la interface fastEthernet 0/0 y la IP interface fastEthernet 0/0.2?

Si, la IP de la interface fastEthernet 0/0 es 172.20.40.1 y la IP de la interface fastEthernet 0/0.2 es 172.20.44.1

Paso 7 – Comprobar la comunicación entre las V-LANs del Switch por medio del Router. Para esto, utilizar el comando ping entre las PCs y contestar las siguientes preguntas:

17. Emita un ping del PC1 a todas las estaciones. ¿El ping fue exitoso?

El ping fue exitoso todas las estaciones de trabajo porque la comunicación entre V-LANs se realiza por medio del Router a nivel de capa 3

4.4 PRÁCTICA DE COMUNICACIÓN ENTRE V-LAN CON DOS SWITCH POR MEDIO DE UN ROUTER

Duración estimada: 75 min.

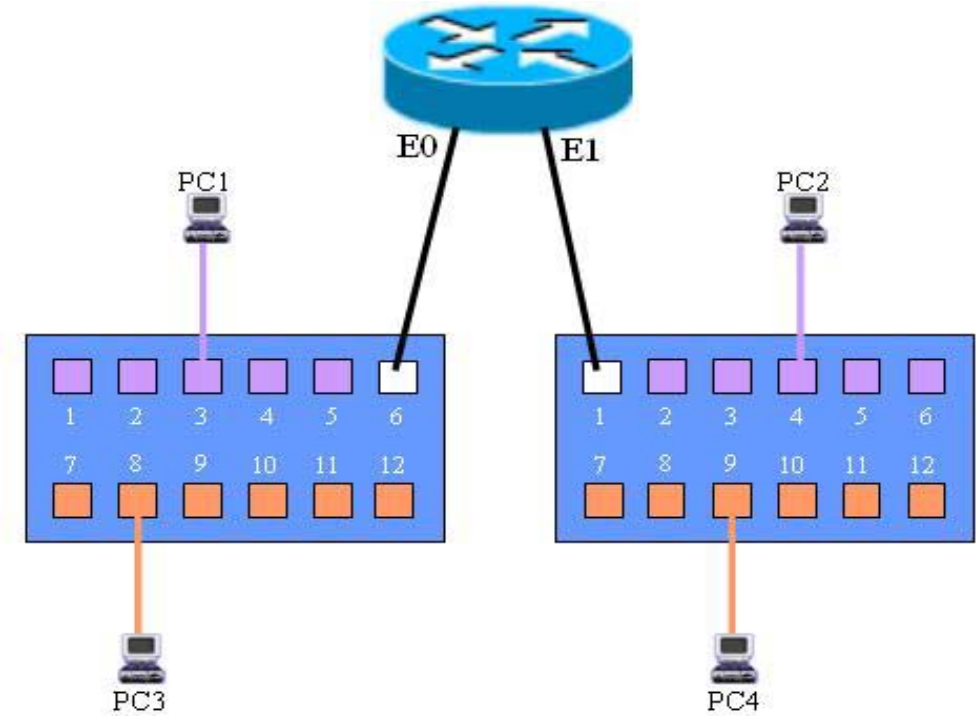


Figura 4.4 V-LAN con dos Switch y un Router

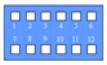
Nombre del Switch 1 : SW-1	Nombre del Switch 2 : SW-2
Tipo de Switch : 2950	Tipo de Switch : 2950
Nombre de V-LAN1 : alumnos	Nombre de V-LAN1 : alumnos
Nombre de V-LAN2 : profesores	Nombre de V-LAN2 : profesores
Puertos para V-LAN1 : 1,2,3,4 y 5	Puertos para V-LAN1 : 1,2,3,4,5 y 6
Puertos para V-LAN2 : 7,8,9,10,11 y 12	Puertos para V-LAN2 : 8,9,10,11 y12
Puerto de Trunk : 6	Puerto de Trunk : 7
IP de los PCs de la V-LAN1 :	IP de los PCs de la V-LAN1 :

172.20.40.(4-8) 255.255.252.0 Puerta de enlace : 172.20.40.1	172.20.40.(9-13) 255.255.252.0 Puerta de enlace : 172.20.40.2
IP de los PCs de la V-LAN2 : 172.20.44.(4-9) 255.255.252.0 Puerta de enlace : 172.20.44.1	IP de los PCs de la V-LAN2 : 172.20.44.(10-15) 255.255.252.0 Puerta de enlace : 172.20.44.2

Nombre del Router : LAB-A
Tipo de Router : 2620
E0/0.1 : 172.20.40.1 255.255.252.0
E0/0.2 : 172.20.44.1 255.255.252.0
E1/0.1 : 172.20.40.2 255.255.252.0
E1/0.2 : 172.20.44.2 255.255.252.0

LEYENDA

 = Router

 = Switch

 = usuarios

= V-LAN1 (alumnos)

= V-LAN2 (profesores)

4.4.1 Objetivos

Esta práctica de laboratorio sirve para practicar las siguientes tareas:

- Conectar a través de la consola al Switch 1 y al Switch 2 para crear y configurar 2 VLANs en cada Switch con sus respectivos nombres
- Probar o hacer ping entre cada uno de los Host conectados a cada V-LAN en cada Switch para verificar la comunicación entre los PCs
- Configurar el enlace Trunk en cada Switch para comunicarse con el Router
- Configurar la fastethernet E0 y E1 del Router para dar soporte a VLAN de cada Switch permitiendo así la intercomunicación entre ellas por medio del Router
- Probar o hacer ping entre cada uno de los Host conectados a cada V-LAN de cada Switch para verificar la intercomunicación entra las V-LANs por medio del Router en la capa 3

4.4.2 Información básica

La implementación de las VLANs se realiza a nivel de capa 2, por lo que pueden ser implementadas en un Switch. La implementación de una VLAN se realiza asignado cada puerto del Switch a una determinada VLAN, limitando la difusión de mensajes entre los dispositivos (puertos) que pertenecen a la misma VLAN. Las VLAN se pueden propagar a través de una jerarquía de Switch pero no pueden propagarse más allá de un Router, ya

que el Router separa por sí mismo dominios de difusión, por lo que no tiene sentido el que las VLAN se propaguen a través de él.

Cuando configuramos un Switch (o grupo de Switches) para que soporte distintas VLANs, es como si en realidad nuestro Switch (o grupo de Switches) lo estuviéramos dividiendo en varias LANs distintas una por cada VLAN. De ahí que necesitemos de un Router para poder intercomunicarlas entre ellas, la comunicación entre dispositivos de una misma VLAN (LAN) se realiza a nivel de capa 2 (direcciones MAC), pero la comunicación entre dispositivos de distintas VLANs (LANs) se realiza a nivel de capa 3 (direcciones IP). Consecuencia de esto es que a cada VLAN se le debe de asignar un espacio de direcciones distinto, debiéndose de realizar subneting en la subred.

4.4.3 Herramientas / preparación

Antes de comenzar con la práctica de laboratorio, el profesor o asistente de laboratorio debe preparar dos Switch con los valores VLAN por defecto, un Router, dos estaciones de trabajo con HyperTerminal para realizar la conexión de consola al Switch y al Router. A continuación se suministra la lista de equipo requerido.

- Dos estaciones de PC con HyperTerminal instalado para configurar el Switch y el Router
- Cuatro estaciones de PC Windows

- Dos Switch Cisco (modelo 2900 Series)
- Un Router Cisco (modelo 2600 Series)
- 2 cables de consola (roll-over) y dos adaptadores DB-9/RJ45 o cables de módem nulo DB-9
- Cable Ethernet CAT 6 desde cada estación de trabajo a un puerto Ethernet de cada Switch

4.4.4 Recursos Web

- LAN Switching basics www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/lanswtch.htm
- General information on all Cisco products - (Ir al capítulo 22 - Switches) www.cisco.com/univercd/cc/td/doc/pcat/#2
- 1900 / 2820 series Ethernet switches www.cisco.com/warp/public/cc/pd/si/casi/ca1900/prodlit/s1928_ov.htm
- 2900 series Fast Ethernet switches www.cisco.com/warp/public/cc/pd/si/casi/ca2900xl/prodlit/s290xl_ov.htm
- 3500 series Gigabit Ethernet switches www.cisco.com/warp/public/cc/pd/si/casi/ca3500/prodlit/s3500x_ov.htm
- Virtual LAN for 1900/2820 Switches www.cisco.com/univercd/cc/td/doc/product/lan/28201900/1928v8x/esc98x/02vlans.htm

- Información general acerca de los routers

  www.cisco.com/univercd/cc/td/doc/pcat/#2

- Routers de la Serie 2500

  www.cisco.com/warp/public/cc/cisco/mkt/access/2500/index.shtml

4.4.5 Notas

4.4.6 Comandos a utilizar en la práctica de comunicación entre VLAN con dos Switch por medio de un Router

- **Comandos en el Switch**

Comandos	Descripción
configure terminal	Entra al modo de configuración global. Realiza la configuración desde la terminal de consola de forma manual
End	Sale del modo de configuración
interface fastEthernet 0/id	Entra a una interface FastEthernet establecidas por el usuario
interface vlan id	Entra a la interface de una V-LAN
ip address	Coloca una dirección ip
Ip default-gateway ip	Coloca una dirección de puerta de enlace
Ping	Utiliza el protocolo ICMP para verificar la conexión de hardware y la dirección lógica en la capa de internet, envía mensajes de eco al dispositivo vecino
show running-config	Muestra el archivo de configuración activo o muestra la configuración

	actual en la RAM
show vlan	Muestra todas la V-LANs con sus respectivos puertos asignados a cada una de ellas
switchport mode access vlan id	Asigna un puerto o un rango de puertos a una V-LAN
Switchport mode trunk	Define un puerto como trunk
Switchport trunk allowed vlan all	Determina que todas las V-LAN del Switch tendrán acceso al puerto trunk
vlan database	Entra al modo de configuración de las VLAN
vlan vlan-id **name** vlan-name	Crea una V-LAN con un número (1-1001) determinado y a la vez le coloca un nombre

Tabla 4.5 Comandos de Swich de la practica de V-LAN

con dos Switch y un Router

- **Comandos en el Router**

Comandos	Descripción
Configure terminal	Realiza la configuración desde la terminal de consola de forma manual
Encapsulation dot1Q 2	Especifica que una interface utiliza un etiquetado de V-LANS basado en el estándar IEEE 802.1Q
interface fastEthernet	Entra a la configuración de la interfaz Ethernet
ip address	Coloca una dirección ip
No shutdown	Habilita la interfaz deseada
Ping	Utiliza el protocolo ICMP para verificar la conexión de hardware y la dirección lógica en la capa de internet, envía mensajes de eco al dispositivo vecino
show interface serial	Muestra estadísticas de la interface serial configurada en el Router
show running-config	Muestra el archivo de configuración activo o muestra la configuración actual en la RAM

Tabla 4.6 Comandos del Router en la practica de V-LAN

con dos Switch y un Router

4.4.7 Pasos para la práctica de práctica de comunicación entre VLAN con dos Switch por medio de un Router

Seleccione un Switch (modelo Cisco 2950 Series), un Router (Modelo 2600 series) y 4 PCs antes de comenzar la práctica de laboratorio. Conectar una estación de trabajo a la conexión del puerto de consola del Switch para configurar cada puerto con su respectiva V-LAN (V-LAN1 y V-LAN2), conectar los 4 computadores al Switch 1 en los puertos 1, 3, 8 y 10, conectar el puerto 12 del Switch con la interfaz FastEthernet 0/0 del Router.

Paso 1 – Utilizar el diagrama de laboratorio, colocar los siguientes comandos para crear V-LANs con el Switch 1 y responda las siguientes preguntas:

SW-1# vlan database

SW-1(vlan)# vlan 2 name profesores

SW-1# show vlan

1. ¿Cuántos puertos están asignados a la V-LAN 1?

_____

2. ¿Cuántos puertos están asignados a la V-LAN 2?

_____

_____

Paso 2 – Configurar la IP y la puerta de enlace para cada V-LAN en el Switch 1, para acceder de manera remota al Router, para esto, utilizar los siguientes comandos y contestar las siguientes preguntas:

SW-1# configure terminal

SW-1(config)# interface vlan 1

SW-1(config-if)# ip address 172.20.40.3 255.255.252.0

SW-1(config-if)# exit

SW-1(config)# interface vlan 1

SW-1(config-if)# ip default-gateway 172.20.40.1

SW-1(config-if)# no shutdown

SW-1(config-if)# end

SW-1# configure terminal

SW-1(config)# interface vlan 2

SW-1(config-if)# ip address 172.20.44.3 255.255.252.0

SW-1(config-if)# exit

SW-1(config)# interface vlan 2

SW-1(config-if)# ip default-gateway 172.20.44.1

SW-1(config-if)# no shutdown

SW-1(config-if)# end

SW-1# show running-config

3. ¿Muestra la IP de la V-LAN 1 y la IP de la V-LAN 2?

4. ¿Muestra la puerta de enlace de la V-LAN 1 y la V-LAN 2?

Paso 3 – Asignar puertos a cada V-LAN en el Switch 1 con los siguientes comandos y contestar las siguientes preguntas:

SW-1# configure terminal

SW-1(config)# interface fastEthernet 0/7

SW-1(config-if)# switchport mode access vlan 2

SW-1(config-if)# end

SW-1# configure terminal

SW-1(config)# interface fastEthernet 0/8

SW-1(config-if)# switchport mode access vlan 2

SW-1(config-if)# end

SW-1# configure terminal

SW-1(config)# interface fastEthernet 0/9

SW-1(config-if)# switchport mode access vlan 2

SW-1(config-if)# end

SW-1# configure terminal

SW-1(config)# interface fastEthernet 0/10

SW-1(config-if)# switchport mode access vlan 2

SW-1(config-if)# end

SW-1# configure terminal

SW-1(config)# interface fastEthernet 0/11

SW-1(config-if)# switchport mode access vlan 2

SW-1(config-if)# end

SW-1# configure terminal

SW-1(config)# interface fastEthernet 0/12

SW-1(config-if)# switchport mode access vlan 2

SW-1(config-if)# end

SW-1# show running-config

5. ¿Cuántas interfaces FastEthernet están asignadas a la V-LAN 1?

_____

6. ¿ Cuántas interfaces FastEthernet están asignadas a la V-LAN 2?

_____

Paso 4 - Probar la funcionalidad de las 2 VLAN en el Switch 1, utilice el comando ping en cada estación de trabajo y contestar las siguientes preguntas:

7. Emita un ping del PC1 a las demás estaciones de trabajo. ¿El ping fue exitoso?

_____

8. Cambie el PC1 del puerto 1 al puerto 7 y emita un ping a la estación PC3. ¿qué ocurrió?

_____

Cambie el PC1 al puerto 3 para seguir con el diagrama inicial.

Paso 5 – Configuración del puerto Trunk en el puerto 6 del Switch 1 con los siguientes comandos y contestar las siguientes preguntas:

SW-1# configure terminal

SW-1(config)# interface fastEthernet 0/6

SW-1(config-if)# switchport mode trunk

SW-1 (config-if)# switchport trunk allowed vlan all

SW-1 (config-if)# end

SW-1# show interfaces fastEthernet 0/6

9. ¿Como esta el modo administrativo de la interfaz del puerto 6?

_____

10. ¿Cuántas V-LANs tienen acceso al puerto Trunk?

_____

Paso 6 – Utilizar el diagrama de laboratorio, colocar los siguientes comandos para crear V-LANs con el Switch 2 y responda las siguientes preguntas:

SW-2# vlan database

SW-2(vlan)# vlan 2 name profesores

SW-2# show vlan

11. ¿Cuántos puertos están asignados a la V-LAN 1?

_____

12. ¿Cuántos puertos están asignados a la V-LAN 2?

_____

_____

Paso 7 – Configurar la IP y la puerta de enlace para cada V-LAN en el Switch 2, para acceder de manera remota al Router, para esto, utilizar los siguientes comandos y contestar las siguientes preguntas:

SW-2# configure terminal

SW-2(config)# interface vlan 1

SW-2(config-if)# ip address 172.20.40.3 255.255.252.0

SW-2(config-if)# exit

SW-2(config)# interface vlan 1

SW-2(config-if)# ip default-gateway 172.20.40.2

SW-2(config-if)# no shutdown

SW-2(config-if)# end

SW-2# configure terminal

SW-2(config)# interface vlan 2

SW-2(config-if)# ip address 172.20.44.3 255.255.252.0

SW-2(config-if)# exit

SW-2(config)# interface vlan 2

SW-2(config-if)# ip default-gateway 172.20.44.2

SW-2(config-if)# no shutdown

SW-2(config-if)# end

SW-2# show running-config

13. ¿Muestra la IP de la V-LAN 1 y la IP de la V-LAN 2?

_____

14. ¿Muestra la puerta de enlace de la V-LAN 1 y la V-LAN 2?

_____

Paso 8 – Asignar puertos a cada V-LAN en el Switch 2 con los siguientes comandos y contestar las siguientes preguntas:

SW-2# configure terminal

SW-2(config)# interface fastEthernet 0/7

SW-2(config-if)# switchport mode access vlan 2

SW-2(config-if)# end

SW-2# configure terminal

SW-2(config)# interface fastEthernet 0/8

SW-2(config-if)# switchport mode access vlan 2

SW-2(config-if)# end

SW-2# configure terminal

SW-2(config)# interface fastEthernet 0/9

SW-2(config-if)# switchport mode access vlan 2

SW-2(config-if)# end

SW-2# configure terminal

SW-2(config)# interface fastEthernet 0/10

SW-2(config-if)# switchport mode access vlan 2

SW-2(config-if)# end

SW-2# configure terminal

SW-2(config)# interface fastEthernet 0/11

SW-2(config-if)# switchport mode access vlan 2

SW-2(config-if)# end

SW-2# configure terminal

SW-2(config)# interface fastEthernet 0/12

SW-2(config-if)# switchport mode access vlan 2

SW-2(config-if)# end

SW-2# show running-config

15. ¿Cuántas interfaces FastEthernet están asignadas a la V-LAN 1?

_____

16. ¿ Cuántas interfaces FastEthernet están asignadas a la V-LAN 2?

_____

Paso 9 - Probar la funcionalidad de las 2 VLAN en el Switch 2, utilice el comando ping en cada estación de trabajo y contestar las siguientes preguntas:

17. Emita un ping del PC2 a las demás estaciones de trabajo. ¿El ping fue exitoso?

_____

_____

18. Cambie el PC2 del puerto 1 al puerto 8 y emita un ping a la estación PC4. ¿qué ocurrió?

_____

_____

Cambie el PC2 al puerto 2 para seguir con el diagrama inicial.

Paso 10 – Configuración del puerto Trunk en el puerto 1 del Switch 2 con los siguientes comandos y contestar las siguientes preguntas:

SW-2# configure terminal

SW-2(config)# interface fastEthernet 0/1

SW-2(config-if)# switchport mode trunk

SW-2 (config-if)# switchport trunk allowed vlan all

SW-2 (config-if)# end

SW-2# show interfaces fastEthernet 0/1

19 . ¿Como esta el modo administrativo de la interfaz del puerto 1?

_____

20. ¿Cuántas V-LANs tienen acceso al puerto Trunk?

Paso 11 – Configurar la comunicación de las V-LANs de los dos Switch en el Router con los siguientes comandos y contestar las siguientes preguntas:

LAB-A# configure terminal

LAB-A(config)# interface fastEthernet 0/0

LAB-A(config-if)# ip address 172.20.40.1 255.255.252.0

LAB-A(config-if)# no shutdown

LAB-A(config-if)# end

LAB-A# configure terminal

LAB-A (config)#interface fastEthernet 0/0.2

LAB-A (config-subif)#encapsulation dot1Q 2

LAB-A (config-subif)#ip address 172.20.44.1 255.255.252.0

LAB-A (config-subif)#exit

LAB-A# configure terminal

LAB-A(config)# interface fastEthernet 0/1

LAB-A(config-if)# ip address 172.20.40.2 255.255.252.0

LAB-A(config-if)# no shutdown

LAB-A(config-if)# end

LAB-A# configure terminal

LAB-A (config)#interface fastEthernet 0/1.2

LAB-A (config-subif)#encapsulation dot1Q 2

LAB-A (config-subif)#ip address 172.20.44.2 255.255.252.0

LAB-A (config-subif)#exit

LAB-A# show running-configure

21. ¿ Muestra la IP de la interface fastEthernet 0/0 y la IP interface fastEthernet 0/0.2?

_____

22. ¿ Muestra la IP de la interface fastEthernet 0/1 y la IP interface fastEthernet 0/1.2?

_____

_____

Paso 12 – Comprobar la comunicación entre la V-LAN 1 del Switch 1 y la V-LAN 1 del Switch 2 por medio del Router y la comunicación entre la VLAN 2 del Switch 1 y la V-LAN 2 del Switch 2 por medio del Router. Para esto, utilizar el comando ping entre las PCs y contestar las siguientes preguntas:

23. Emita un ping del PC1 al PC2 y al PC4. ¿El ping fue exitoso?

_____

_____

24. Emita un ping del PC4 al PC1 y al PC3. ¿El ping fue exitoso?

_____

_____

Paso 13 – Configurar la comunicación de V-LAN en el Router con los siguientes comandos y contestar las siguientes preguntas:

LAB-A# configure terminal

LAB-A(config)# interface fastEthernet 0/0

LAB-A(config-if)# ip address 172.20.40.1 255.255.252.0

LAB-A(config-if)# no shutdown

LAB-A(config-if)# end

LAB-A# configure terminal

LAB-A (config)#interface fastEthernet 0/0.2

LAB-A (config-subif)#encapsulation dot1Q 2

LAB-A (config-subif)#ip address 172.20.44.1 255.255.252.0

LAB-A (config-subif)#exit

LAB-A# show running-configure

25. ¿ Muestra la IP de la interface fastEthernet 0/0 y la IP interface fastEthernet 0/0.2?

_____

_____

Paso 14 – Comprobar la comunicación entre las V-LANs del Switch por medio del Router. Para esto, utilizar el comando ping entre las PCs y contestar las siguientes preguntas:

26. Emita un ping del PC1 a todas las estaciones. ¿El ping fue exitoso?

_____

_____

4.4.8 Respuestas de la práctica de comunicación entre V-LAN con dos Switch por medio de un Router

Paso 1 – Utilizar el diagrama de laboratorio, colocar los siguientes comandos para crear V-LANs con el Switch 1 y responda las siguientes preguntas:

SW-1# vlan database

SW-1(vlan)# vlan 2 name profesores

SW-1# show vlan

1. ¿Cuántos puertos están asignados a la V-LAN 1?

Todos los puertos pertenecen a la V-LAN 1 (alumnos)

2. ¿Cuántos puertos están asignados a la V-LAN 2?

Ninguno, porque no se ha configurado los puertos del Switch para la VLAN 2, sólo se le coloco el nombre profesores a una posible V-LAN 2.

Paso 2 – Configurar la IP y la puerta de enlace para cada V-LAN en el Switch 1, para acceder de manera remota al Router, para esto, utilizar los siguientes comandos y contestar las siguientes preguntas:

SW-1# configure terminal

SW-1(config)# interface vlan 1

SW-1(config-if)# ip address 172.20.40.3 255.255.252.0

SW-1(config-if)# exit

SW-1(config)# interface vlan 1

SW-1(config-if)# ip default-gateway 172.20.40.1

SW-1(config-if)# no shutdown

SW-1(config-if)# end

SW-1# configure terminal

SW-1(config)# interface vlan 2

SW-1(config-if)# ip address 172.20.44.3 255.255.252.0

SW-1(config-if)# exit

SW-1(config)# interface vlan 2

SW-1(config-if)# ip default-gateway 172.20.44.1

SW-1(config-if)# no shutdown

SW-1(config-if)# end

SW-1# show running-config

3. ¿Muestra la IP de la V-LAN 1 y la IP de la V-LAN 2?

Si, IP de la V-LAN 1 es 172.20.40.3 y la IP de la V-LAN 2 es 172.20.44.3

4. ¿Muestra la puerta de enlace de la V-LAN 1 y la V-LAN 2?

Si, la puerta de enlace de la V-LAN 1 es 172.20.40.1 y de la V-LAN 2 es 172.20.44.1

Paso 3 – Asignar puertos a cada V-LAN en el Switch 1 con los siguientes comandos y contestar las siguientes preguntas:

SW-1# configure terminal

SW-1(config)# interface fastEthernet 0/7

SW-1(config-if)# switchport mode access vlan 2

SW-1(config-if)# end

SW-1# configure terminal

SW-1(config)# interface fastEthernet 0/8

SW-1(config-if)# switchport mode access vlan 2

SW-1(config-if)# end

SW-1# configure terminal

SW-1(config)# interface fastEthernet 0/9

SW-1(config-if)# switchport mode access vlan 2

SW-1(config-if)# end

SW-1# configure terminal

SW-1(config)# interface fastEthernet 0/10

SW-1(config-if)# switchport mode access vlan 2

SW-1(config-if)# end

SW-1# configure terminal

SW-1(config)# interface fastEthernet 0/11

SW-1(config-if)# switchport mode access vlan 2

SW-1(config-if)# end

SW-1# configure terminal

SW-1(config)# interface fastEthernet 0/12

SW-1(config-if)# switchport mode access vlan 2

SW-1(config-if)# end

SW-1# show running-config

5. ¿Cuántas interfaces FastEthernet están asignadas a la V-LAN 1?

Seis, desde la FastEthernet 0/1 hasta la FastEthernet 0/6

6. ¿ Cuántas interfaces FastEthernet están asignadas a la V-LAN 2?

Seis, desde la FastEthernet 0/7 hasta la FastEthernet 0/12

Paso 4 - Probar la funcionalidad de las 2 VLAN en el Switch 1, utilice el comando ping en cada estación de trabajo y contestar las siguientes preguntas:

7. Emita un ping del PC1 a las demás estaciones de trabajo. ¿El ping fue exitoso?

El ping no fue exitoso en la estación de trabajo PC3 porque no pertenece a la misma V-LAN 1.

8. Cambie el PC1 del puerto 1 al puerto 7 y emita un ping a la estación PC3. ¿qué ocurrió?

El ping fue exitoso en la estación de trabajo PC3 porque pertenecen a la misma V-LAN 2.

Cambie el PC1 al puerto 3 para seguir con el diagrama inicial.

Paso 5 – Configuración del puerto Trunk en el puerto 6 del Switch 1 con los siguientes comandos y contestar las siguientes preguntas:

SW-1# configure terminal
SW-1(config)# interface fastEthernet 0/6
SW-1(config-if)# switchport mode trunk
SW-1 (config-if)# switchport trunk allowed vlan all
SW-1 (config-if)# end
SW-1# show interfaces fastEthernet 0/6

9. ¿Como esta el modo administrativo de la interfaz del puerto 6?

Esta configurado como Trunk

10. ¿Cuántas V-LANs tienen acceso al puerto Trunk?

Todas las V-LANs

Paso 6 – Utilizar el diagrama de laboratorio, colocar los siguientes comandos para crear V-LANs con el Switch 2 y responda las siguientes preguntas:

SW-2# vlan database

SW-2(vlan)# vlan 2 name profesores

SW-2# show vlan

11. ¿Cuántos puertos están asignados a la V-LAN 1?

Todos los puertos pertenecen a la V-LAN 1 (alumnos)

12. ¿Cuántos puertos están asignados a la V-LAN 2?

Ninguno, porque no se ha configurado los puertos del Switch para la VLAN 2, sólo se le coloco el nombre profesores a una posible V-LAN 2.

Paso 7 – Configurar la IP y la puerta de enlace para cada V-LAN en el Switch 2, para acceder de manera remota al Router, para esto, utilizar los siguientes comandos y contestar las siguientes preguntas:

SW-2# configure terminal

SW-2(config)# interface vlan 1

SW-2(config-if)# ip address 172.20.40.3 255.255.252.0

SW-2(config-if)# exit

SW-2(config)# interface vlan 1

SW-2(config-if)# ip default-gateway 172.20.40.2

SW-2(config-if)# no shutdown

SW-2(config-if)# end

SW-2# configure terminal

SW-2(config)# interface vlan 2

SW-2(config-if)# ip address 172.20.44.3 255.255.252.0

SW-2(config-if)# exit

SW-2(config)# interface vlan 2

SW-2(config-if)# ip default-gateway 172.20.44.2

SW-2(config-if)# no shutdown

SW-2(config-if)# end

SW-2# show running-config

13. ¿Muestra la IP de la V-LAN 1 y la IP de la V-LAN 2?

Si, IP de la V-LAN 1 es 172.20.40.3 y la IP de la V-LAN 2 es 172.20.44.3

14. ¿Muestra la puerta de enlace de la V-LAN 1 y la V-LAN 2?

Si, la puerta de enlace de la V-LAN 1 es 172.20.40.2 y de la V-LAN 2 es 172.20.44.2

Paso 8 – Asignar puertos a cada V-LAN en el Switch 2 con los siguientes comandos y contestar las siguientes preguntas:

SW-2# configure terminal

SW-2(config)# interface fastEthernet 0/7

SW-2(config-if)# switchport mode access vlan 2

SW-2(config-if)# end

SW-2# configure terminal

SW-2(config)# interface fastEthernet 0/8

SW-2(config-if)# switchport mode access vlan 2

SW-2(config-if)# end

SW-2# configure terminal

SW-2(config)# interface fastEthernet 0/9

SW-2(config-if)# switchport mode access vlan 2

SW-2(config-if)# end

SW-2# configure terminal

SW-2(config)# interface fastEthernet 0/10

SW-2(config-if)# switchport mode access vlan 2

SW-2(config-if)# end

SW-2# configure terminal

SW-2(config)# interface fastEthernet 0/11

SW-2(config-if)# switchport mode access vlan 2

SW-2(config-if)# end

SW-2# configure terminal

SW-2(config)# interface fastEthernet 0/12

SW-2(config-if)# switchport mode access vlan 2

SW-2(config-if)# end

SW-2# show running-config

15. ¿Cuántas interfaces FastEthernet están asignadas a la V-LAN 1?

Seis, desde la FastEthernet 0/1 hasta la FastEthernet 0/6

16. ¿ Cuántas interfaces FastEthernet están asignadas a la V-LAN 2?

Seis, desde la FastEthernet 0/7 hasta la FastEthernet 0/12

Paso 9 - Probar la funcionalidad de las 2 VLAN en el Switch 2, utilice el comando ping en cada estación de trabajo y contestar las siguientes preguntas:

17. Emita un ping del PC2 a las demás estaciones de trabajo. ¿El ping fue exitoso?

El ping no fue exitoso en la estación de trabajo PC4 porque no pertenece a la misma V-LAN 1.

18. Cambie el PC2 del puerto 1 al puerto 8 y emita un ping a la estación PC4. ¿qué ocurrió?

El ping fue exitoso en la estación de trabajo PC4 porque pertenecen a la misma V-LAN 2.

Cambie el PC2 al puerto 2 para seguir con el diagrama inicial.

Paso 10 – Configuración del puerto Trunk en el puerto 1 del Switch 2 con los siguientes comandos y contestar las siguientes preguntas:

SW-2# configure terminal

SW-2(config)# interface fastEthernet 0/1

SW-2(config-if)# switchport mode trunk

SW-2 (config-if)# switchport trunk allowed vlan all

SW-2 (config-if)# end

SW-2# show interfaces fastEthernet 0/1

19 . ¿Como esta el modo administrativo de la interfaz del puerto 1?

Esta configurado como Trunk

20. ¿Cuántas V-LANs tienen acceso al puerto Trunk?

Todas las V-LANs

Paso 11 – Configurar la comunicación de las V-LANs de los dos Switch en el Router con los siguientes comandos y contestar las siguientes preguntas:

LAB-A# configure terminal

LAB-A(config)# interface fastEthernet 0/0

LAB-A(config-if)# ip address 172.20.40.1 255.255.252.0

LAB-A(config-if)# no shutdown

LAB-A(config-if)# end

LAB-A# configure terminal

LAB-A (config)#interface fastEthernet 0/0.2

LAB-A (config-subif)#encapsulation dot1Q 2

LAB-A (config-subif)#ip address 172.20.44.1 255.255.252.0

LAB-A (config-subif)#exit

LAB-A# configure terminal

LAB-A(config)# interface fastEthernet 0/1

LAB-A(config-if)# ip address 172.20.40.2 255.255.252.0

LAB-A(config-if)# no shutdown

LAB-A(config-if)# end

LAB-A# configure terminal

LAB-A (config)#interface fastEthernet 0/1.2

LAB-A (config-subif)#encapsulation dot1Q 2

LAB-A (config-subif)#ip address 172.20.44.2 255.255.252.0

LAB-A (config-subif)#exit

LAB-A# show running-configure

21. ¿ Muestra la IP de la interface fastEthernet 0/0 y la IP interface fastEthernet 0/0.2?

Si, la IP de la interface fastEthernet 0/0 es 172.20.40.1 y la IP de la interface fastEthernet 0/0.2 es 172.20.44.1

22. ¿ Muestra la IP de la interface fastEthernet 0/1 y la IP interface fastEthernet 0/1.2?

Si, la IP de la interface fastEthernet 0/1 es 172.20.40.2 y la IP de la interface fastEthernet 0/1.2 es 172.20.44.2

Paso 12 – Comprobar la comunicación entre la V-LAN 1 del Switch 1 y la V-LAN 1 del Switch 2 por medio del Router y la comunicación entre la VLAN 2 del Switch 1 y la V-LAN 2 del Switch 2 por medio del Router. Para esto, utilizar el comando ping entre las PCs y contestar las siguientes preguntas:

23. Emita un ping del PC1 al PC2 y al PC4. ¿El ping fue exitoso?

El ping fue exitoso todas las estaciones de trabajo porque la comunicación entre V-LANs se realiza por medio del Router a nivel de capa 3

24. Emita un ping del PC4 al PC1 y al PC3. ¿El ping fue exitoso?

El ping fue exitoso todas las estaciones de trabajo porque la comunicación entre V-LANs se realiza por medio del Router a nivel de capa 3

5. PRÁCTICAS DE VPN

5.1 PRÁCTICA DE PPP COMO FUNCIONAMIENTO BÁSICO DE VPN EN EL ROUTER

Duración estimada: 45 minutos

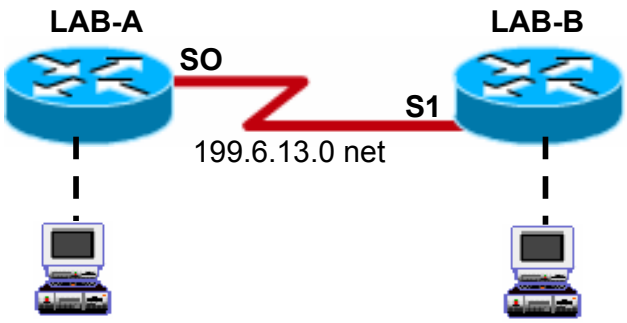


Figura 5.1 Comunicación de dos Router con PPP

Nombre del Router : LAB-A	Nombre del Router : LAB-B
Tipo de Router : 2620	Tipo de Router : 2620
SO : 199.6.13.1	S1 : 199.6.13.2
Máscara de S0: 255.255.255.0	Máscara de S0: 255.255.255.0
Interfaz: DCE	Interfaz: DTE

LEYENDA

 = Router

 = Consola

- - - = Cable de consola

5.1.1 Objetivos

- Manipular correctamente el uso de dos Routers para configurar protocolos WAN
- Comprender cómo afectan a las conexiones seriales, el protocolo punto a punto PPP de encapsulamiento WAN
- Entender el funcionamiento de PPP como herramienta para la implementación de redes privadas virtuales (VPN)
- Verificar la autenticación CHAP en los Routers

5.1.2 Información básica

El enfoque de esta práctica de Laboratorio se centra en PPP (Protocolo punto a punto). PPP es un protocolo de red de área amplia (WAN) que proporciona servicios de capa 2 del modelo OSI para las conexiones Router a Router y host a red a través de circuitos utilizando una interfaz serial. PPP se considera parte del conjunto de protocolo TCP/IP y soporta una cantidad de protocolos LAN, como IP e IPX, y diversos métodos de autenticación de seguridad, como PAP y CHAP. PPP se puede utilizar en

diversos medios físicos, incluyendo cable de par trenzado, fibra o transmisión satelital. PPP utiliza el Control de enlace de datos de alto nivel (HDLC) como base para encapsulación de datagramas. PPP es un protocolo muy importante en las VPNs porque hace posible la utilización de túneles.

Al configurar los enlaces WAN seriales para la práctica de Laboratorio del Router, el encapsulamiento de capa 2 por defecto es una versión propietaria de Cisco del protocolo de control de enlace de datos de alto nivel (HDLC). Con esta práctica de Laboratorio, convertirá los enlaces WAN entre los routers de Laboratorio de HDLC a PPP. Se debe establecer el encapsulamiento PPP en ambos extremos de la conexión WAN y configurar en encapsulamiento CHAP en uno de los Routers.

5.1.3 Herramientas / preparación

Antes de comenzar esta práctica de Laboratorio, el profesor o el ayudante de Laboratorio deben tener la configuración de nombres y claves del Laboratorio estándar de 2 routers. Se trabaja individualmente o en equipos. A continuación, presentamos una lista de los recursos requeridos.

- Configuración de Laboratorio estándar de 2 routers de Cisco.
- 2 routers con enlace WAN entre ellos y encapsulamiento HDLC (por defecto).
- 2 estaciones de trabajo, conectadas al puerto de consola de cada Router.
- Manuales del Router.

5.1.4 Recursos Web

- Información básica sobre enrutamiento

  www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/routing.htm
- Información general acerca de los routers

  www.cisco.com/univercd/cc/td/doc/pcat/#2
- Routers de la Serie 2500

  www.cisco.com/warp/public/cc/cisco/mkt/access/2500/index.shtml
- Routers de la Serie 1600

  www.cisco.com/warp/public/cc/cisco/mkt/access/1600/index.shtml
- Terminología y siglas

  www.cisco.com/univercd/cc/td/doc/cisintwk/ita/index.htm
- Resumen de los comandos de IOS para el protocolo

  www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cgcr/rbkixol.htm
- Introducción a las tecnologías WAN

  www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/introwan.htm

5.1.5 Notas

5.1.5 Comandos a utilizar en la práctica de PPP

Comandos	Descripción
Bandwidth	Sobrescribe el ancho de banda predeterminado
configure terminal	Realiza la configuración desde la terminal de consola de forma manual
encapsulation ppp	Activa el encapsulamiento del protocolo punto a punto en el Router
interface serial	Entra a la configuración de la interfaz deseada
Ping	Utiliza el protocolo ICMP para verificar la conexión de hardware y la dirección lógica en la capa de internet, envía mensajes de eco al dispositivo vecino
ppp authentication chap	Activa la autenticación CHAP
show cdp neighbors	Visualiza las actualizaciones de cdp en el Router local o las plataformas y protocolos en los dispositivos vecinos
show interface serial	Muestra estadísticas de la interface serial configurada en el Router
show running-config	Muestra el archivo de configuración activo o muestra la configuración actual en la RAM

Tabla 5.1 Comandos del Router para la práctica de PPP

5.1.7 Pasos para la configuración de PPP

Seleccione un par de routers que tengan un enlace serial WAN entre ellos, LAB-A con la conexión DCE y LAB-B con la conexión DTE, antes de comenzar la práctica de Laboratorio. Conecte una estación de trabajo a la conexión del puerto de consola del primer Router (LAB-A) y otra estación de trabajo al segundo Router (LAB-B).

Paso 1 - Utilizar el diagrama de laboratorio y el comando show running-config en el Router LAB-A para contestar las siguientes preguntas:

LAB-A# show running-config

1. ¿Cuál es el ancho de banda que se ha establecido para esta interfaz (si es que se ha establecido alguno)?

Paso 2 - Utilizar el comando show interface para contestar las siguientes preguntas:

LAB-A# show interfaces serial 0/0

2. ¿Cuál es el estado de la interfaz y del protocolo de línea?

---

3. ¿En qué valor se establece actualmente el encapsulamiento?

Paso 3 - Eliminar la configuración del ancho de banda de Serial S0 utilizando el siguiente conjunto de comandos:

LAB-A# configure terminal

LAB-A(config)# interface serial 0/0

LAB-A(config-if)# no bandwidth

4. Utilice el comando show interface s0/0 nuevamente. ¿En qué valor se establece actualmente el ancho de banda?

Paso 4 - Utilizar el comando show cdp neighbors para verificar la conexión con el Router vecino:

LAB-A# show cdp neighbors

5. ¿Puede ver el nombre, la intefaz y el modelo del Router vecino?

Paso 5 – En el Router LAB-B, Utilizar el comando show interface y contestar las siguientes preguntas:

LAB-B# show interfaces serial 0/1

6. ¿Cuál es el estado de la interfaz y del protocolo de línea?

---

7. ¿En qué valor se establece actualmente el encapsulamiento?

Paso 6 - Cambiar el encapsulamiento WAN en Router LAB-A de HDLC a PPP y configurar la autenticación CHAP

Utilice los siguientes comandos para definir el nombre de usuario y la contraseña del Router remoto, donde el nombre es el nombre del host remoto (LAB-B) y secreto es la contraseña (practica) que debe ser la misma en ambos Routers. Configurar el encapsulamiento PPP en el Router LAB-A, la autenticación CHAP, y conteste las siguientes preguntas:

LAB-A(config)# username nombre **password** secreto

LAB-A(config)# interface serial 0/0

LAB-A(config-if)# encapsulation ppp

LAB-A(config-if)#ppp authentication chap

8. Utilice el comando show interface serial 0/0. ¿Cuál es el estado de la interfaz y del protocolo de línea?

---

9. ¿Qué significa esto?

---

10. ¿En qué valor se establece actualmente el encapsulamiento?

---

11. ¿Puede hacer ping desde Router LAB-A a Router LAB-B?

---

12. ¿Por qué o por qué no?

Paso 7 - Cambiar el encapsulamiento WAN en Router LAB-B de HDLC a PPP

Utilice los siguientes comandos para definir el nombre de usuario y la contraseña del Router remoto, donde el nombre es el nombre del host remoto (LAB-A) y secreto es la contraseña (practica) que debe ser la misma en ambos Routers. Configurar el encapsulamiento PPP en el Router LAB-B y conteste las siguientes preguntas:

LAB-B# configure terminal

LAB-B(config)#username nombre **password** secreto

LAB-B(config)# interface serial 0/1

LAB-B(config-if)# encapsulation ppp

13. Utilice el comando show interface serial 0/1. ¿Cuál es el estado de la interfaz y del protocolo de línea?

---

14. ¿En qué valor se establece actualmente el encapsulamiento?

---

15. ¿Puede hacer ping desde Router LAB-A a Router LAB-B?

---

16. ¿Por qué o por qué no?

5.1.8 Respuestas de la práctica de PPP

Paso 1 - Utilizar el diagrama de laboratorio y el comando show running-config en el Router LAB-A para contestar las siguientes preguntas:

LAB-A# show running-config

1. ¿Cuál es el ancho de banda que se ha establecido para esta interfaz (si es que se ha establecido alguno)?

56 Kbit (para la métrica de enrutamiento)

Paso 2 - Utilizar el comando show interface para contestar las siguientes preguntas:

LAB-A# show interfaces serial 0/0

2. ¿Cuál es el estado de la interfaz y del protocolo de línea?

Serial 0 is up, Line Protocol is up

3. ¿En qué valor se establece actualmente el encapsulamiento?

HDLC (propietario de Cisco - por defecto)

Paso 3 - Eliminar la configuración del ancho de banda de Serial S0 utilizando el siguiente conjunto de comandos:

LAB-A# configure terminal

LAB-A(config)# interface serial 0/0

LAB-A(config-if)# no bandwidth

4. Utilice el comando show interface s0/0 nuevamente. ¿En qué valor se establece actualmente el ancho de banda?

1544 Kbit, enlace de datos WAN digital más común.

Paso 4 - Utilizar el comando show cdp neighbors para verificar la conexión con el Router vecino:

LAB-A# show cdp neighbors

5. ¿Puede ver el nombre, la intefaz y el modelo del Router vecino?

Si

Paso 5 – En el Router LAB-B, Utilizar el comando show interface y contestar las siguientes preguntas:

LAB-B# show interfaces serial 0/1

6. ¿Cuál es el estado de la interfaz y del protocolo de línea?

Serial 1 is up, Line Protocol is up

7. ¿En qué valor se establece actualmente el encapsulamiento?

HDLC (propietario de Cisco - por defecto)

Paso 6 - Cambiar el encapsulamiento WAN en Router LAB-A de HDLC a PPP y configurar la autenticación CHAP

Utilice los siguientes comandos para definir el nombre de usuario y la contraseña que del Router remoto, donde el nombre es el nombre del host remoto (LAB-B) y secreto es la contraseña (practica) que debe ser la misma en ambos Routers. Configurar el encapsulamiento PPP en el Router LAB-A, la autenticación CHAP, y conteste las siguientes preguntas:

LAB-A(config)# username nombre **password** secreto

LAB-A(config)# interface serial 0/0

LAB-A(config-if)# encapsulation ppp

LAB-A(config-if)#ppp authentication chap

8. Utilice el comando show interface serial 0/0. ¿Cuál es el estado de la interfaz y del protocolo de línea?

Serial 1 is up, Line Protocol is down

9. ¿Qué significa esto?

El enlace físico (cable) de Capa 1 está OK, pero los protocolos de enlace de datos de Capa 2 no se comunican (no reciben mensajes de actividad)

10. ¿En qué valor se establece actualmente el encapsulamiento?

PPP

11. ¿Puede hacer ping desde Router LAB-A a Router LAB-B?

No

12. ¿Por qué o por qué no?

El encapsulamiento WAN en LAB-A Serial 0 actualmente es PPP y el encapsulamiento WAN en LAB-B Serial 1 todavía sigue siendo la opción por defecto, HDLC. Estos son dos protocolos de enlace de datos WAN distintos y no son compatibles.

Paso 7 - Cambiar el encapsulamiento WAN en Router LAB-B de HDLC a PPP

Utilice los siguientes comandos para definir el nombre de usuario y la contraseña del Router remoto, donde el nombre es el nombre del host remoto (LAB-A) y secreto es la contraseña (practica) que debe ser la misma

en ambos Routers. Configurar el encapsulamiento PPP en el Router LAB-B y conteste las siguientes preguntas:

LAB-B# configure terminal

LAB-B(config)#username nombre **password** secreto

LAB-B(config)# interface serial 0/1

LAB-B(config-if)# encapsulation ppp

13. Utilice el comando show interface serial 0/1. ¿Cuál es el estado de la interfaz y del protocolo de línea?

Serial 0 is up, Line Protocol is up

14. ¿En qué valor se establece actualmente el encapsulamiento?

PPP

15. ¿Puede hacer ping desde Router LAB-A a Router LAB-B?

Sí

16. ¿Por qué o por qué no?

El encapsulamiento WAN en LAB-A Serial 0 y LAB-B Serial 1 actualmente está establecido con el mismo protocolo de enlace de datos (PPP).

5.2 PRÁCTICA DE CONFIGURACIÓN DE VPN EN WINDOWS 2000 SERVER

Duración estimada: 75 minutos

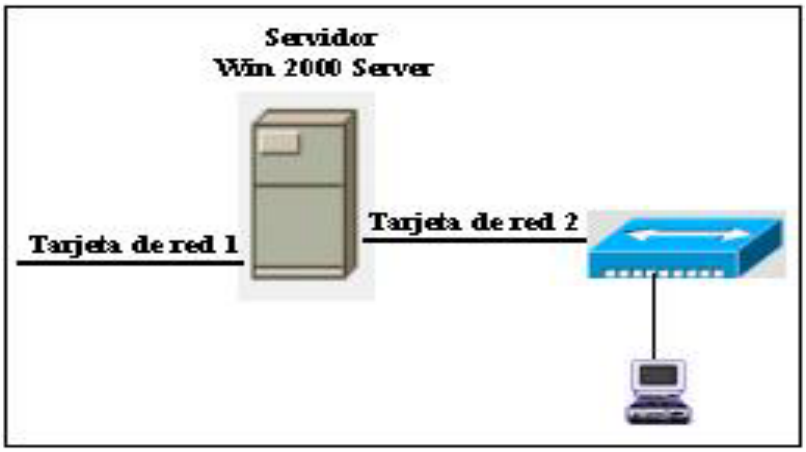
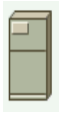


Figura 5.2 Topología para VPN con Windows 2.000 Server

Nombre del Servidor : servidor
Tarjeta de red 1 IP : 162.20.40.2 Máscara : 255.255.252.0 Puerta de Enlace : 162.20.40.1
Tarjeta de red 2 IP : 172.20.40.2 Máscara : 255.255.0.0 Puerta de Enlace : 172.20.40.1

Nombre del PC : laboratorio
IP : 172.20.40.12 Máscara de red : 255.255.0.0 Puerta de Enlace : 172.20.40.1

LEYENDA

 =Servidor

 = HUB

 = PC

5.2.1 Objetivos

- Configurar un servidor de dominios, agregar usuarios al dominio, configurar el cliente para acceder al servidor de dominios, con el fin de establecer todos los parámetros básicos para la configuración de VPN.
- Afirmar los conceptos de VPN por medio de una configuración con Windows 2.000 Server (en el PC Servidor) y Windows 2.000 Profesional (en los usuarios).
- Manipular y configurar correctamente todos los recursos que ofrece Windows 2.000 Server y Windows 2.000 Profesional para la implementación de VPN.
- Comprender como afecta una VPN en una red local
- Entender el funcionamiento de VPN como herramienta para la implementación de redes seguras a bajo costo.
- Verificar la autenticación y la certificación en el cliente y el servidor.
- Verificar los diferentes protocolos de túneles que implementa Windows 2.000 Server para realizar conexiones VPN.

5.2.2 Información básica

En esta práctica de laboratorio, se trabaja la configuración de VPN por medio de la utilidad o recursos que ofrece Windows 2.000 Server. Una red privada virtual (VPN, Virtual Private Network) es la extensión de una red privada que incluye vínculos de redes compartidas o públicas. Con una red privada virtual, se puede enviar datos entre dos equipos a través de una red mediante un vínculo privado punto a punto.

Para realizar un vínculo punto a punto, los datos se encapsulan o empaquetan con un encabezado que proporciona la información de enrutamiento que permite a los datos recorrer la red compartida o pública hasta alcanzar su destino. Para hacer un vínculo privado, los datos se cifran para asegurar la confidencialidad. Los paquetes interceptados en la red compartida o pública no se pueden descifrar si no se dispone de las claves de cifrado. El vínculo en el que se encapsulan y cifran los datos privados es una conexión de red privada virtual (VPN).

Desde la perspectiva del usuario, la red privada virtual es una conexión punto a punto entre el equipo (el cliente VPN) y el servidor de la organización (el servidor VPN). La infraestructura exacta de la red compartida o pública es irrelevante dado que lógicamente parece como si los datos se enviaran a través de un vínculo privado dedicado.

Las organizaciones también pueden utilizar VPN para establecer conexiones enrutadas con oficinas alejadas geográficamente o con otras organizaciones a través de una red pública al mismo tiempo que realizan comunicaciones seguras.

En esta práctica, se implementa los siguientes tipos de tecnología VPN en Windows 2.000:

- Protocolo de túnel punto a punto (PPTP, Point-to-Point Tunneling Protocol): PPTP utiliza métodos de autenticación de Protocolo punto a punto (PPP) de nivel de usuario.
- Protocolo de túnel de capa 2 (L2TP, Layer Two Tunneling Protocol)) con seguridad de protocolo Internet (IPSec): L2TP utiliza métodos de autenticación de PPP de nivel de usuario y certificados de nivel de equipo con IPSec para cifrar los datos.
- Directivas de acceso remoto: Proporciona al administrador de la red más flexibilidad a la hora de configurar permisos de acceso y atributos de la conexión. Puede exigir el uso de autenticación y cifrado sólido.
- CHAP (Protocolo de autenticación de saludo Challenge): CHAP se utiliza para verificar periódicamente la identidad del nodo remoto. Esto se realiza durante el establecimiento inicial del enlace y se puede repetir en cualquier momento una vez que se ha establecido el enlace. CHAP envía un Challenge, que consiste en una identificación de sesión. El cliente

remoto deberá utilizar el algoritmo de control unidireccional MD5 para devolver el nombre del usuario y una encriptación del Challenge, la identificación de la sesión y la contraseña del cliente. CHAP protege contra la personificación de un cliente al enviar de manera impredecible challenges repetidos al cliente a todo lo largo de la duración de la conexión.

- MS-CHAP (Microsoft Challenge Handshake Authentication Protocol): Windows 2000 incluye compatibilidad con el Protocolo de autenticación por desafío mutuo de Microsoft MS-CHAP, también conocido como MS-CHAP versión 1. MS-CHAP es un protocolo de autenticación de contraseñas de cifrado no reversible. El proceso de desafío mutuo funciona de la manera siguiente:

  1. El autenticador (el servidor de acceso remoto o el servidor IAS) envía al cliente de acceso remoto un desafío formado por un identificador de sesión y una cadena de desafío arbitraria.
  2. El cliente de acceso remoto envía una respuesta que contiene el nombre de usuario y un cifrado no reversible de la cadena de desafío, el identificador de sesión y la contraseña.
  3. El autenticador comprueba la respuesta y, si es válida, se autentican las credenciales del usuario.

- MS-CHAP versión 2: El Protocolo de autenticación por desafío mutuo de Microsoft (MS-CHAP, Microsoft Challenge Handshake Authentication Protocol) versión 2 refuerza significativamente la seguridad de la

transferencia de credenciales de seguridad y la generación de claves de cifrado durante la negociación de una conexión de acceso remoto.

Antes de instalar el servicio de VPN en Windows 2.000 Server, se debe instalar el servidor de dominios en el servidor para que pueda correr la configuración de VPN.

Un servidor de dominio, es un equipo que funciona con Windows 2000 Server, que administra el acceso de los usuarios a una red; esto incluye los inicios de sesión, autenticación y el acceso a los recursos compartido y de directorio.

5.2.3 Herramientas / preparación

Antes de comenzar esta práctica de Laboratorio, el profesor o el ayudante de Laboratorio deben tener la configuración del PC servidor y el PC cliente. Se trabaja individualmente o en equipos. A continuación, presentamos una lista de los recursos requeridos.

- Un PC con Windows 2.000 Server que tenga 2 tarjeta de red
- Un PC con Windows 2.000 Profesional
- Un Hub
- Cables Ethernet CAT 6 desde las estaciones de trabajo a un puerto Ethernet del Hub

5.2.4 Recursos Web

- Información básica sobre enrutamiento

  www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/routing.htm

- Terminología y siglas

  www.cisco.com/univercd/cc/td/doc/cisintwk/ita/index.htm

- Introducción a las tecnologías WAN

  www.cisco.com/univercd/cc/td/doc/cisintwk/ito_doc/introwan.htm

- lro9798/vpn.htm
- lro9798/ungla.dit.upm.es/~pepe/ec/05f-vpn.pdf
- http://www.conecsion.es/soporte.htm
- http://www.linuxware.com.mx/vpn.php
- http://www.conecsion.es/sat/draytek/vpns/pasoapaovpn_archivos/vpn1.htm
- http://www.conecsion.es/sat/draytek/vpns/pasoapaovpns.htm
- http://infoacceso.upv.es/accpub/winxp/WinXP.htm
- http://www.cisco.com/en/US/netsol/ns110/ns170/ns171/ns27/networking_solutions_package.html
- http://www.cisco.com/en/US/netsol/ns110/ns170/net_solution_home.html

5.2.5 Notas

5.2.6 Pasos para crear un servidor de dominio, en Windows 2.000 Server.

Paso 1 - Abrir "Mi PC" → Ir a Panel de Control →

Herramientas Administrativas →

Configurar el servidor→

Aparece la siguiente ventana, dar habilitar Active Directory:

Figura 5.3 Configurar el servidor

Paso 2 – En la ventana de Active Directory, habilitar la opción "iniciar".

Figura 5.4 Active Directory

Active Directory permite que un usuario inicie sesiones en equipos y dominios con una identidad que se puede autenticar y autorizar para tener acceso a los recursos del dominio. Cada usuario que se conecta a la red debe tener su propia cuenta de usuario y su propia contraseña única. Las cuentas de usuario también se pueden usar como cuentas de servicio para algunas aplicaciones.

Paso 3 - Muestra un asistente para crear el Controlador de dominios.

En la siguiente ventana, habilitar la opción "Controlador de dominio para un nuevo dominio" .

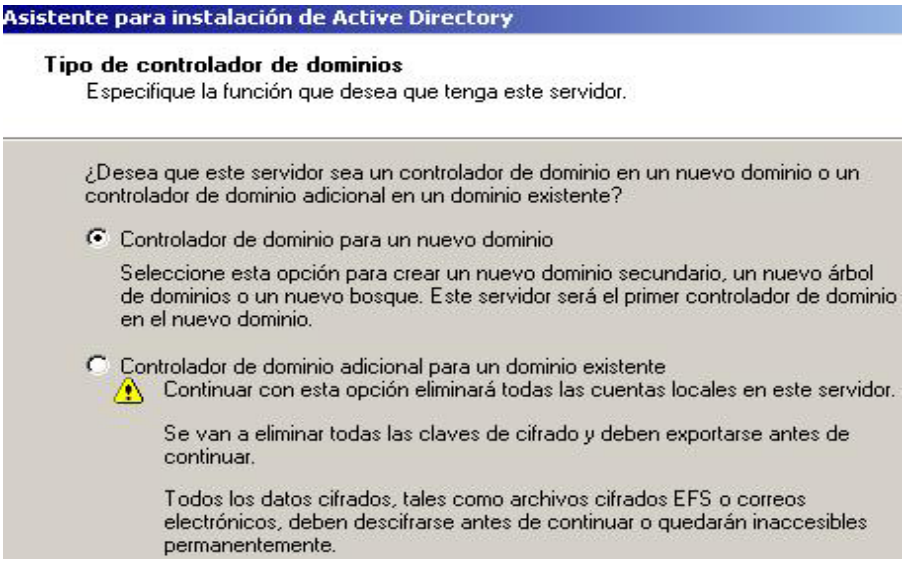


Figura 5.5 Tipo de controlador de dominios

Paso 4 - En la siguiente ventana, habilitar la opción "Crear un nuevo árbol de dominio".

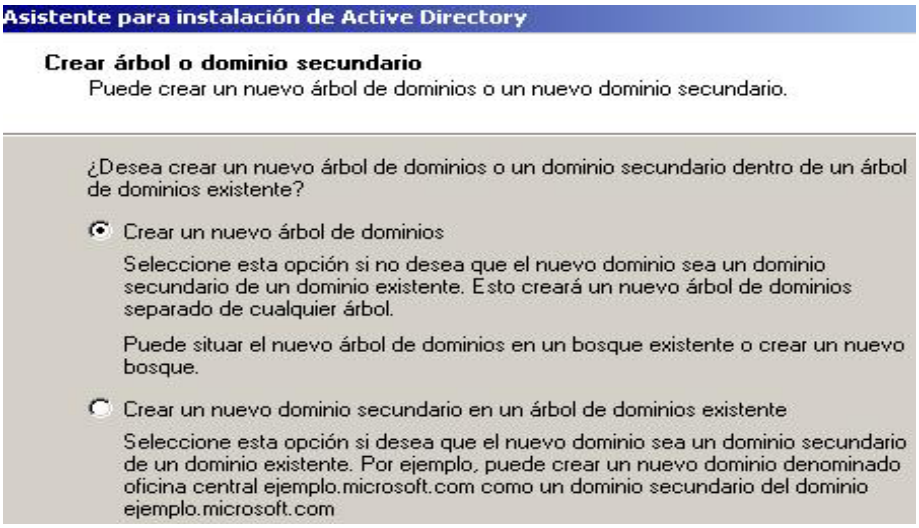


Figura 5.6 Crear árbol de dominio

Paso 5 - En la siguiente ventana, habilitar la opción "Crear un nuevo bosque de árboles de dominio".

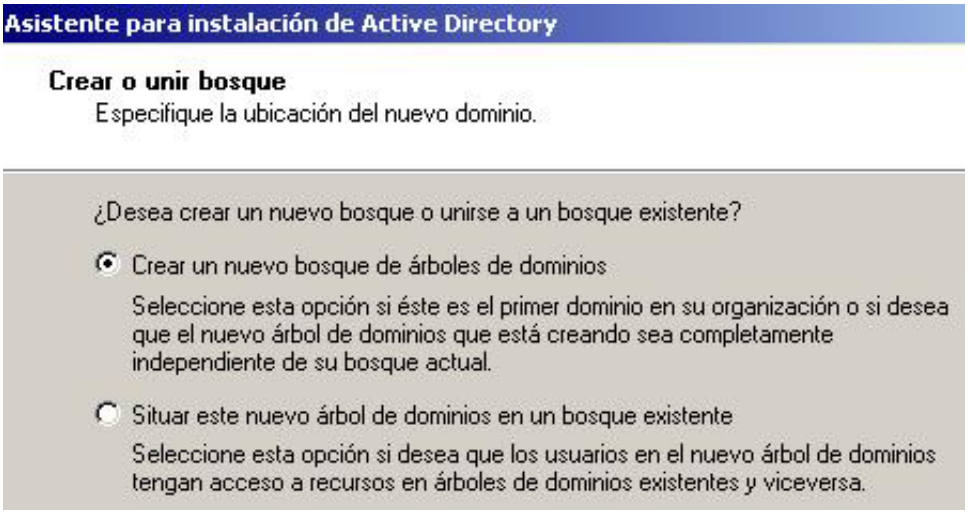


Figura 5.7 Crear o unir bosque

Paso 6 - En la siguiente ventana, digitar el nombre del dominio, para la practica usaremos: vpn.com

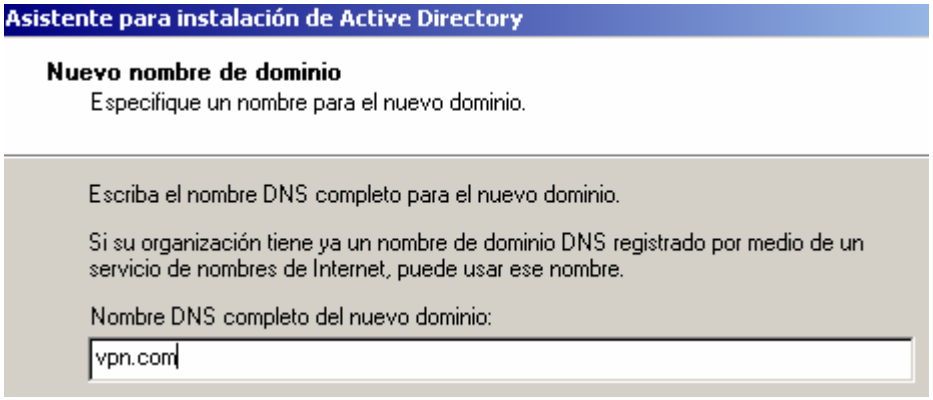


Figura 5.8 Nuevo nombre de dominio

Paso 7 - En la siguiente ventana, digitar el nombre de dominio NetBios, para la usaremos: VPN

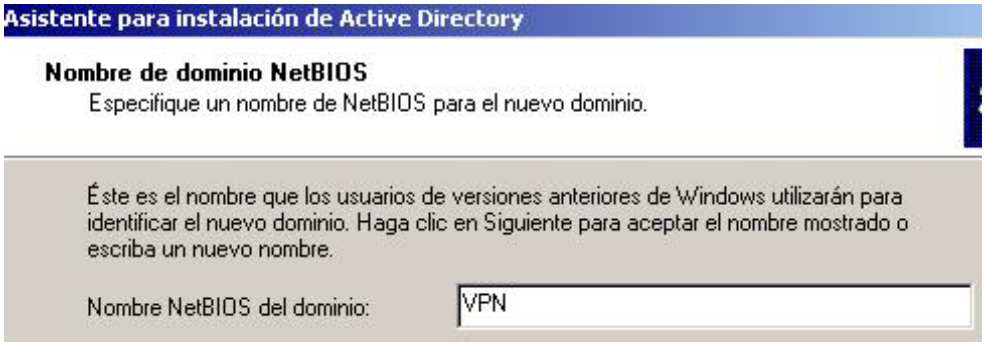


Figura 5.9 Nombre de dominio NetBios

Paso 8- En la siguiente ventana, habilitar la opción "Sí, instalar y configurar DNS".

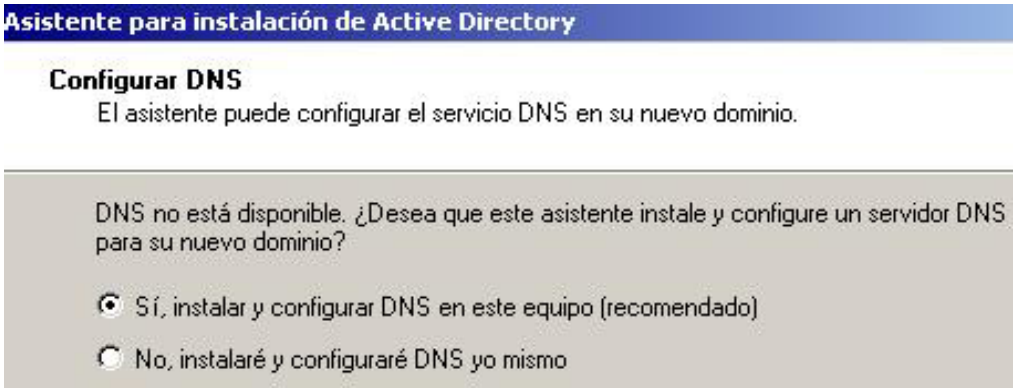


Figura 5.10 Configurar DNS

Paso 9 - En la siguiente ventana, digitar la contraseña del administrador del servidor de dominios.

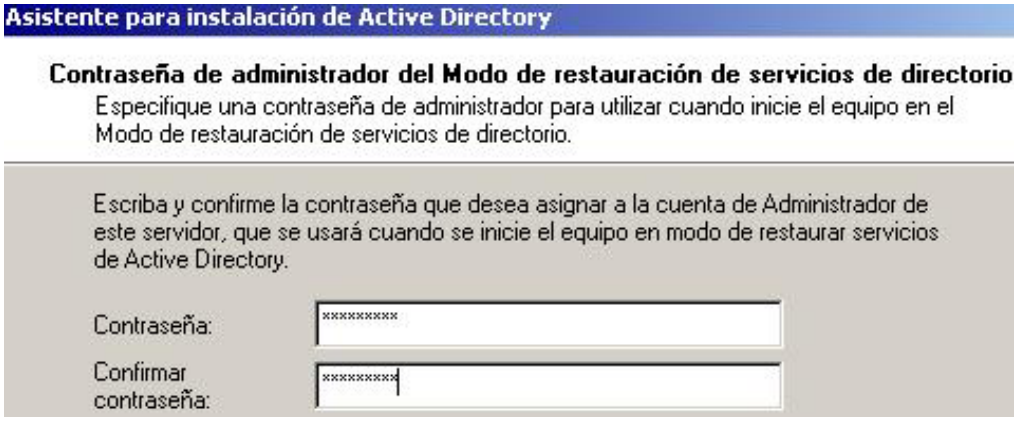


Figura 5.11 Contraseña de administrador

Paso 10 - En la ventana Resumen, dar clic en siguiente y finalizar.

5.2.7 Pasos para la agregar usuarios en un servidor de dominio, en Windows 2.000 Server.

Paso 1 - Abrir "Mi PC" → Ir a Panel de Control →

Herramientas Administrativas → 

Configurar el servidor→ 

Paso 2 – En la ventana de Active Directory, habilitar la opción "iniciar".

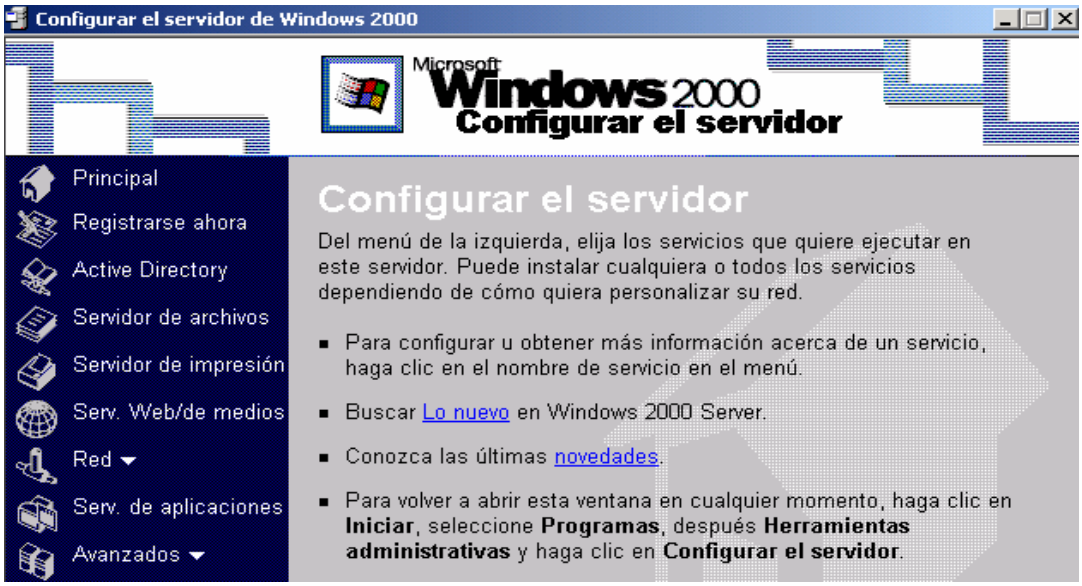


Figura 5.12 Configurar el servidor

Paso 3 - En la ventana de Active Directory, habilitar la opción "Administrar" para crear usuarios.

Figura 5.13 Administrar Active Directory

Paso 4 - En dominio Vpn.com -> clic derecho en User -> Nuevo -> Usuario

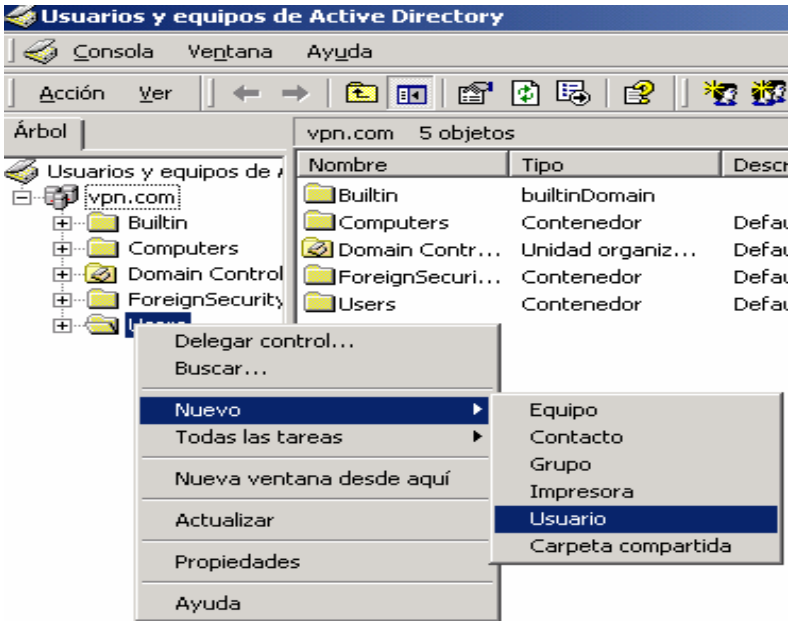


Figura 5.14 Creación de un nuevo usuario

Paso 5 - Digitar el nombre, apellidos y el nombre de inicio de sesión del usuario y hacer clic en siguiente.

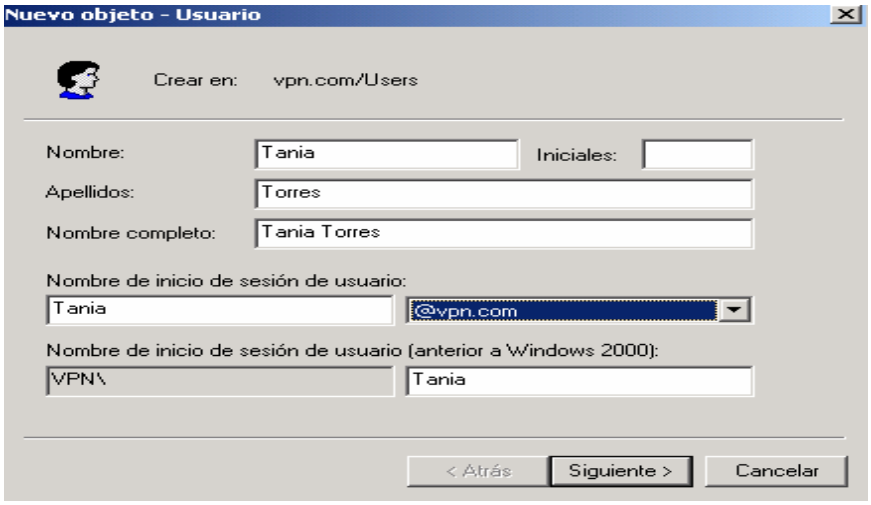


Figura 5.15 Nuevo usuario

Paso 6 -Digitar la contraseña del usuario y habilitamos la opción "El usuario no puede cambiar la contraseña".

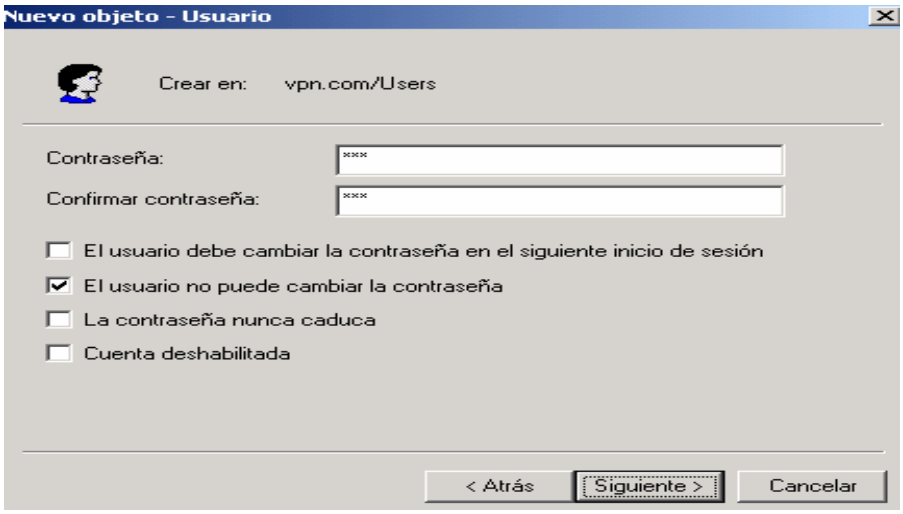


Figura 5.16 Contraseña

Paso 7 - Confirmación de la creación del cliente y damos clic en finalizar para crear el objeto.

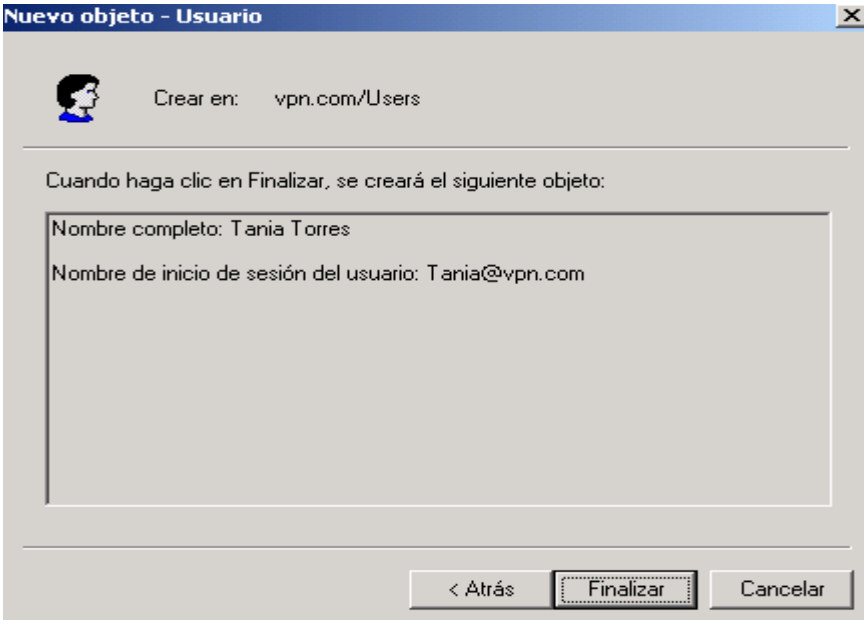


Figura 5.17 Finalizar creación de usuario

Paso 8 - En la carpeta "User" se puede observar el usuario creado. Dar clic en propiedades.

Figura 5.18 Propiedades del usuario

Paso 9 – En la siguiente ventana, en la propiedad de marcado, habilitar "permitir acceso" y dar clic en "Aceptar".

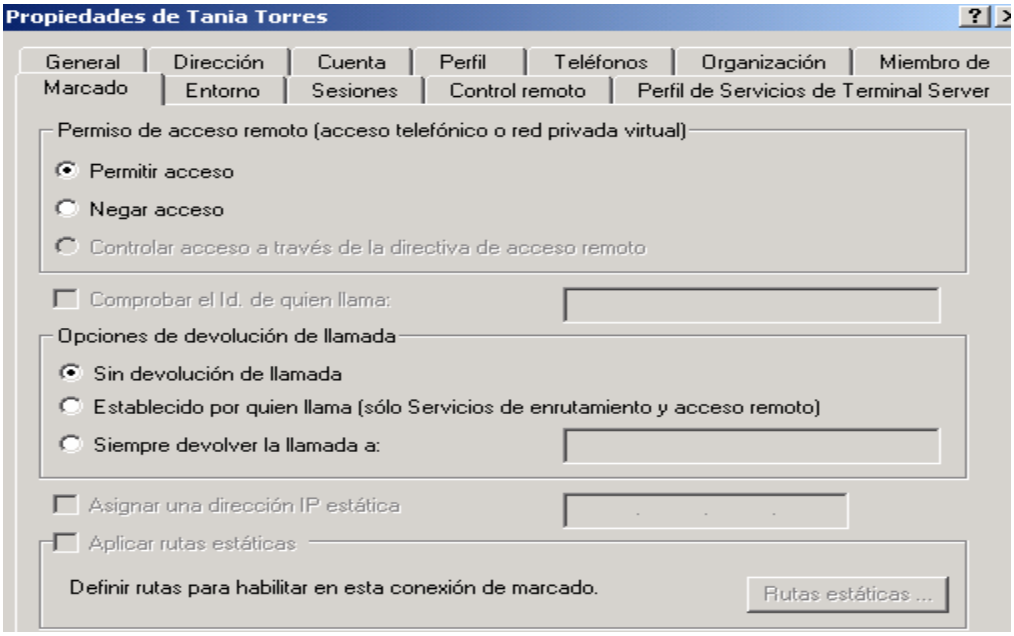


Figura 5.19 Propiedad de marcado

5.2.8 Pasos para la configuración de un usuario Windows 2000 Professional, en el dominio del servidor Windows 2.000 Server.

Paso 1 – Clic derecho en "Mi PC" → Propiedades → Identificación de red → Id de red

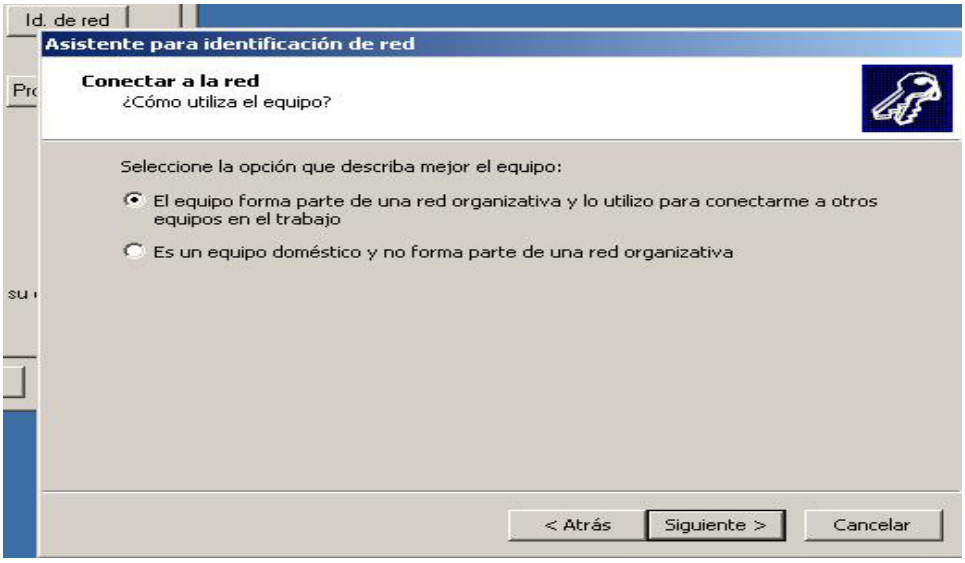


Figura 5.20 Conectar a la red

Paso 2 – En esta ventana muestra un asistente de identificación de red.

Figura 5.21 Asistente para identificación de red

En esta ventana del asistente elegir "Mi organización utiliza una red con un dominio"

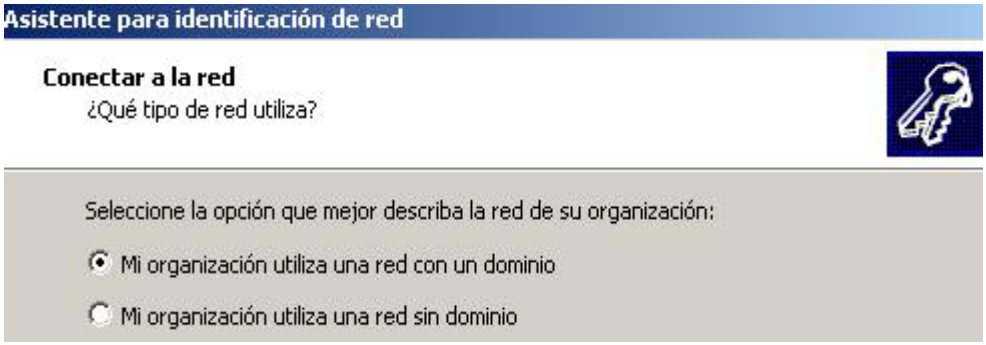


Figura 5.22 Conectar a la red

Paso 3 – En esta ventana en digitar nombre de usuario y el dominio al que quiere pertenecer. Para esta practica digitar VPN.

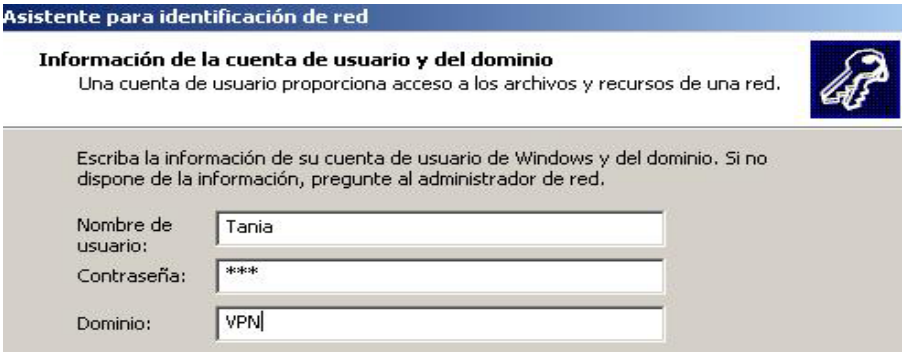


Figura 5.23 Información de la cuenta de usuario

Paso 4 – En esta ventana en digitar nombre del dominio al que quiere pertenecer el equipo. Para esta practica digitar VPN.

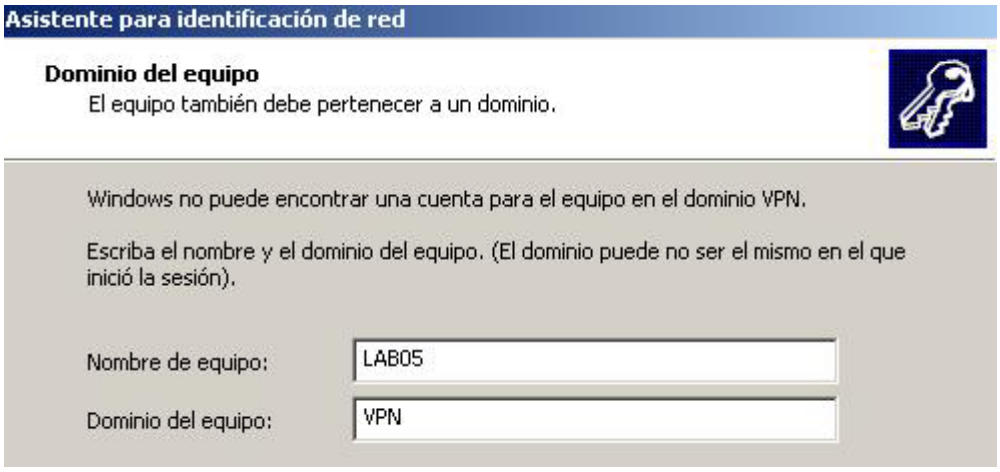


Figura 5.24 Dominio del equipo

Paso 5– En esta ventana en digitar nombre de un nuevo usuario y el dominio al que quiere pertenecer. Para esta practica digitar VPN.

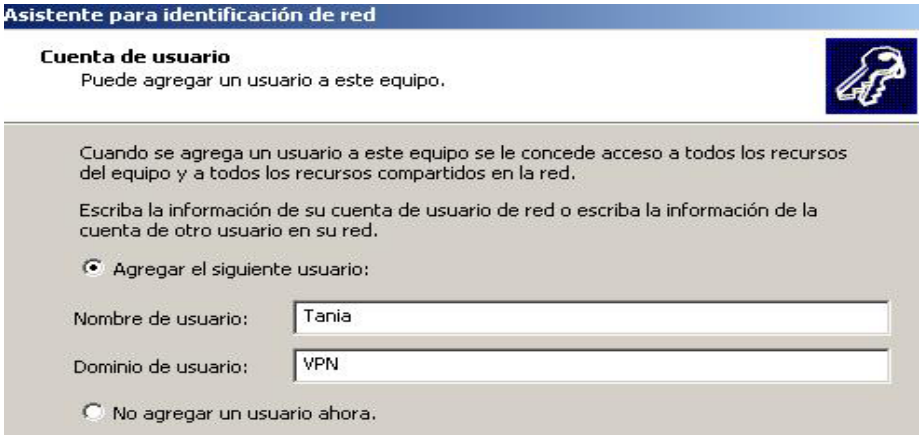


Figura 5.25 Agregar usuario

Paso 6 – En esta ventana en habilitar la opción "Usuario estándar".

Figura 5.26 Nivel de acceso

Paso 7 – En la siguiente ventana del asistente dar clic en finalizar.

Paso 8 – En la ventana "Identificación de red" dar clic en "Id de red".

Figura 5.27 Propiedades del sistema

Paso 9– En la siguiente ventana habilitar la opción "Más".

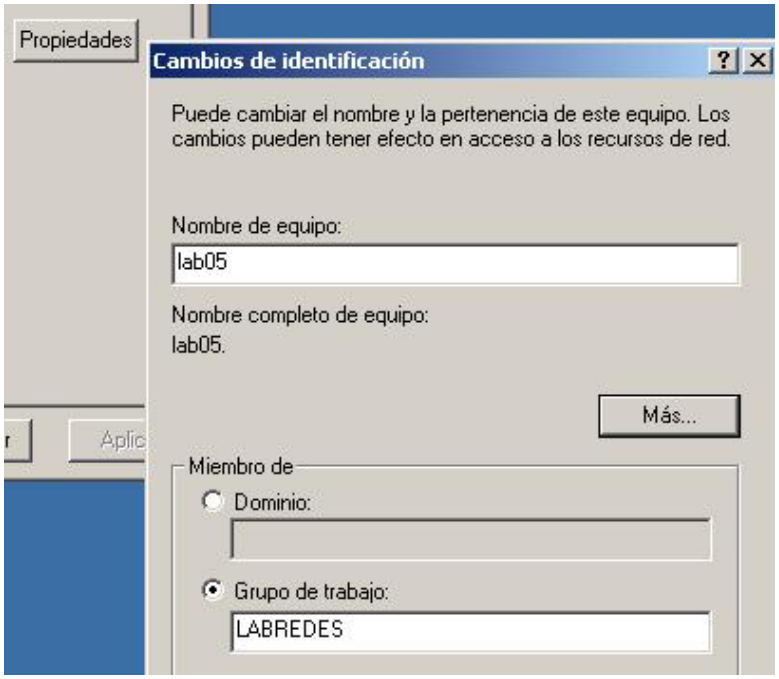


Figura 5.28 Cambios de identificación

Paso 10 – En la siguiente ventana digitar en "sufijo principal DNS de este equipo" vpn.com y dar clic en Aceptar.

Figura 5.29 Cambios de identificación

Paso 11 – En la siguiente ventana en "miembro de" , habilitar "Dominio", digitar vpn.com

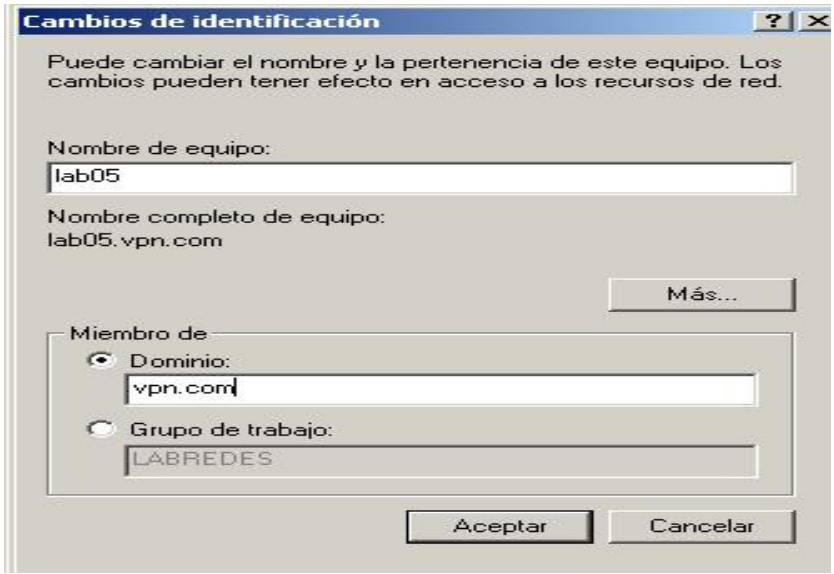


Figura 5.30 Miembro de dominio

5.2.9 Pasos para la configuración del servicio VPN en Windows 2.000 Server

Utilizar el diagrama del laboratorio, y configurar el servidor Windows 2.000 Server de la siguiente forma :

Paso 1 - Abrir "Mi PC" → Ir a Panel de Control →

Herramientas Administrativas → 

Enrutamiento y Acceso Remoto → 

Se accede a "Herramientas administrativas" porque Windows Server, es el que administra la red. Accedemos a "enrutamiento remoto" porque ofrece todas las opciones para enrutar redes.

Paso 2 – En la ventana de Enrutamiento y acceso remoto, dar clic derecho en "Estado del servidor" y clic en "Agregar servidor".

Figura 5.31 Estado del servidor

Se agrega un servidor para que administre la comunicación entre los PCs de la red, aplicando seguridad, rango de direcciones IP de los PCs, servicios y otras opciones de administración de redes.

En esta ventana, agregar el servidor como "Este equipo"

Figura 5.32 Agregar servidor

Se elige "Este equipo" porque se instalará el servicio de VPN en este PC local.

Paso 3 – En esta ventana (figura 5.5), en el servidor creado, dar clic derecho y escoger la opción "Configurar y habilitar el enrutamiento y acceso remoto"

Figura 5.33 Configurar y habilitar el enrutamiento y acceso remoto

Se habilita la opción "Configurar y habilitar el enrutamiento y el acceso remoto" para crear el servidor de red privada virtual.

El asistente permite seleccionar entre varias configuraciones comunes. Una de estas, es habilitar todos los equipos para que se conecten a la red de la práctica. Se selecciona la opción "Servidor de red privada virtual (VPN).

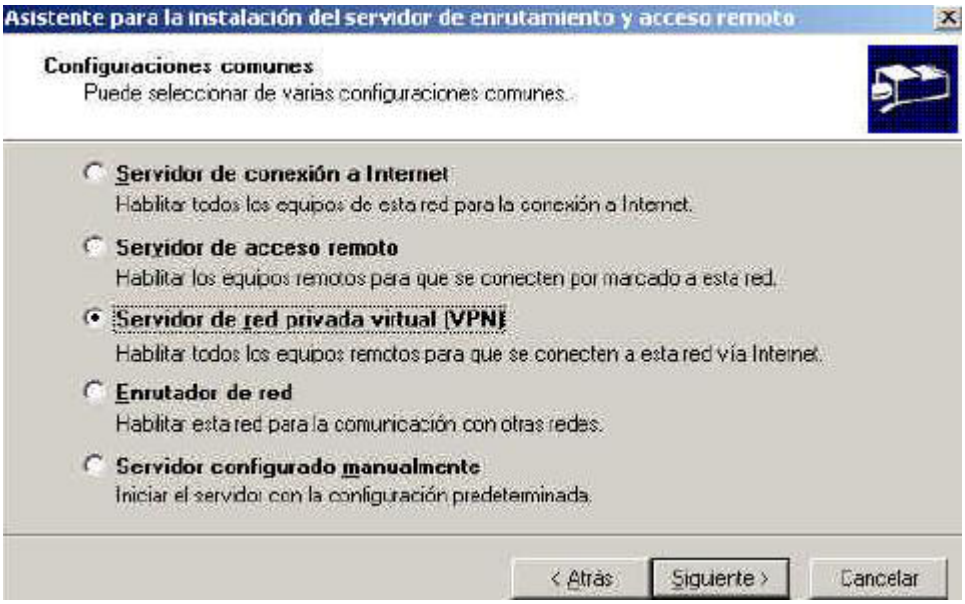


Figura 5.34 Configuraciones comunes

Un servidor de red privada virtual (VPN), puede configurar el servidor VPN para proporcionar acceso a toda la red o restringir el acceso a los recursos del servidor VPN.

Los protocolos necesarios para el acceso VPN deben estar disponibles en el servidor. El asistente nos permite la selección de los mismos en la opción "Protocolos de cliente remoto".

Los protocolos de acceso remoto se utilizan para negociar conexiones y proporcionar el entramado para los datos del protocolo LAN que se envían a través de los enlaces de la red. El acceso remoto de Windows 2000 Server, admite protocolos de LAN como TCP/IP, IPX, AppleTalk, NetBEUI, Novell NetWare, etc. Para las conexiones VPN, el acceso remoto de Windows 2000 Server admite el protocolo de acceso remoto PPP.

Paso 4 – En la siguiente ventana habilitar "Si todos los protocolos"

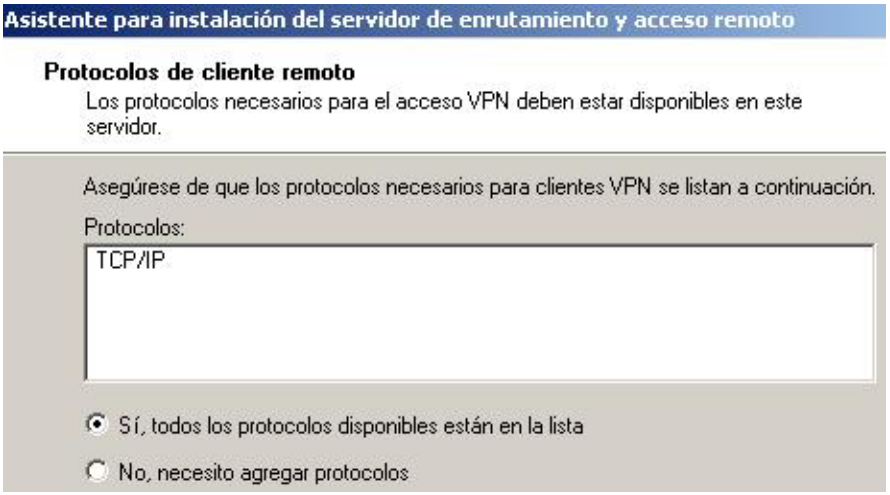


Figura 5.35 Protocolos de cliente remoto

Paso 5 – El asistente muestra el tipo de conexión (Internet o LAN) que usará el servidor. Los clientes VPN remotos y los enrutadores usan una conexión única para tener acceso al servidor. Para esta practica, elegir la conexión de área local y la tarjeta de red 2 (172.20.40.2) como entrada y salida de la LAN hacia la otra tarjeta de red 1 (162.20.40.2).

Dar clic en la conexión LAN y tarjeta de red 2. En esta ventana, se selecciona la asignación de direcciones IP a clientes remotos.

Para esta práctica, elegir "De un intervalo de direcciones especificado"

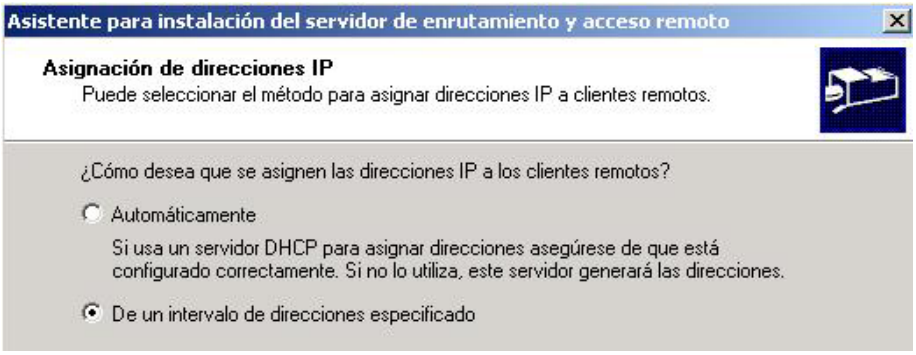


Figura 5.36 Asignación de direcciones IP

En esta ventana se habilita la opción de colocar un rango de IP para los equipos de la red. Para la práctica, colocar el intervalo de dirección IP inicial: 172.20.40.10 y dirección IP final: 172.20.40.50.

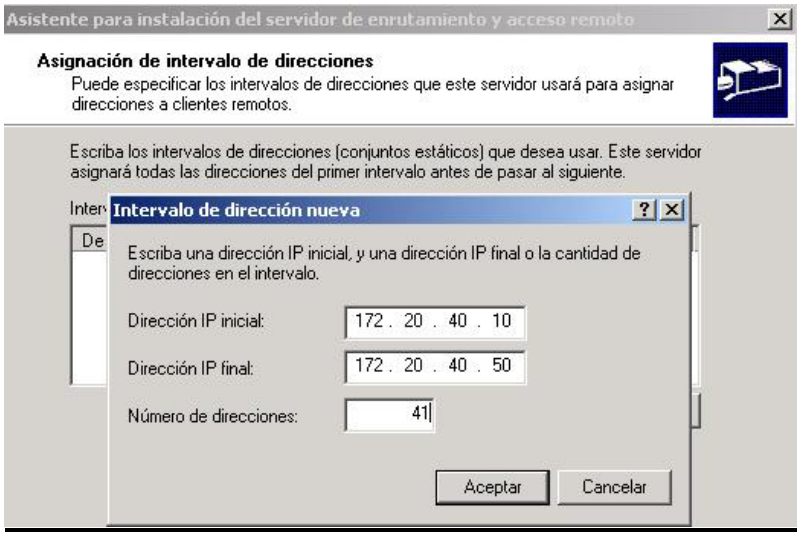


Figura 5.37 Asignación de intervalo de direcciones

Para que el servidor de acceso remoto reenvíe el tráfico correctamente en la red, debe configurarse como un enrutador con rutas estáticas o protocolos de enrutamiento de manera que se pueda tener acceso a todas las ubicaciones de la red desde el servidor de acceso remoto.

Paso 6 – El asistente nos da la opción de instalar un servidor RADIUS.

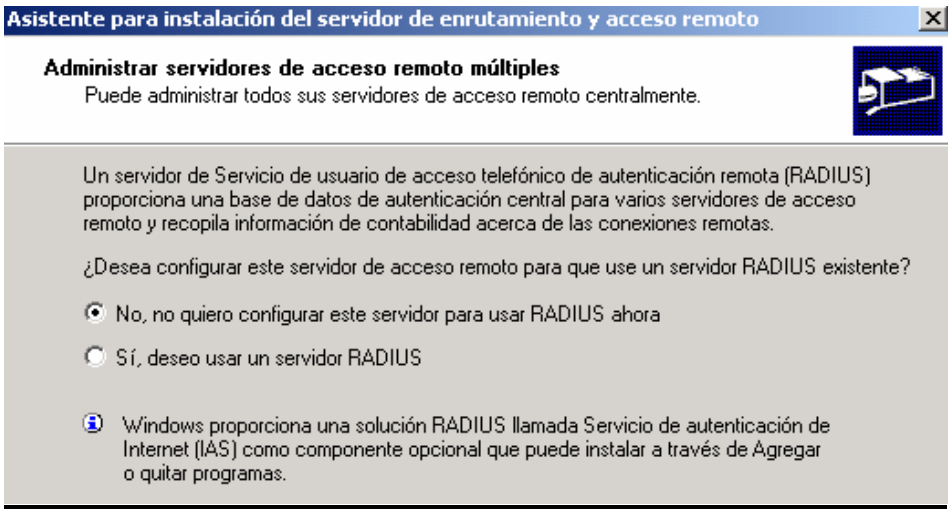


Figura 5.38 Administrar servidores de acceso remoto

Para esta práctica no se instalará el servidor RADIUS, porque ningún usuario de la red implementada accede al servidor por medio de acceso telefónico.

Paso 7 – Terminado toda la configuración anterior, el servidor esta listo para recibir peticiones de VPN.

En el icono de "SERVIDOR (local)", elegir la opción "puertos" y dar click derecho en "Propiedades".

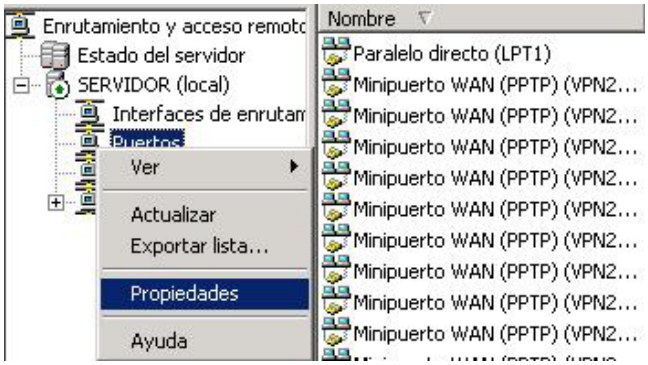


Figura 5.39 Configuración de Puertos en el servidor local

En esta ventana, elegir el protocolo de túnel a utilizar. Para la práctica, elegir el protocolo (PPTP).

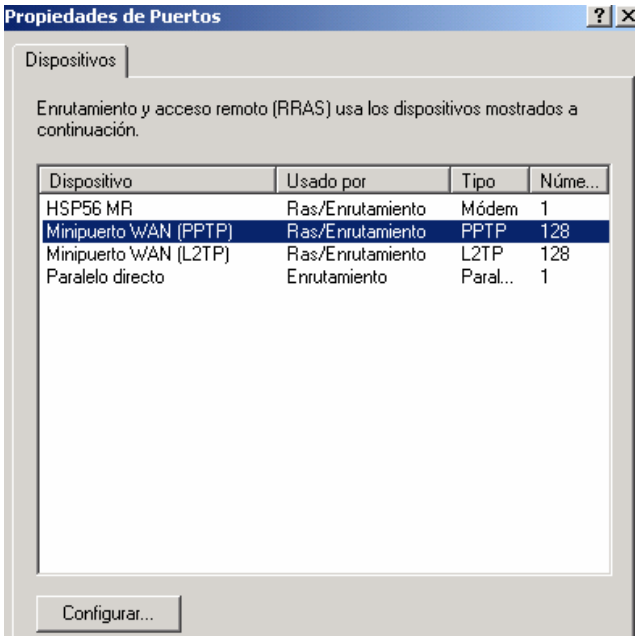


Figura 5.40 Propiedades de Puertos

Los clientes VPN utilizan los protocolos de túnel para crear conexiones seguras a un servidor VPN. Windows 2000 Server incluye los protocolos de túnel PPTP y L2TP.

Paso 8 – Terminado toda la configuración anterior, en el icono de "SERVIDOR (local)", dar clic derecho y elegir la opción "Propiedades". Muestra una ventana (figura 5.12), donde se elige la opción "Seguridad".

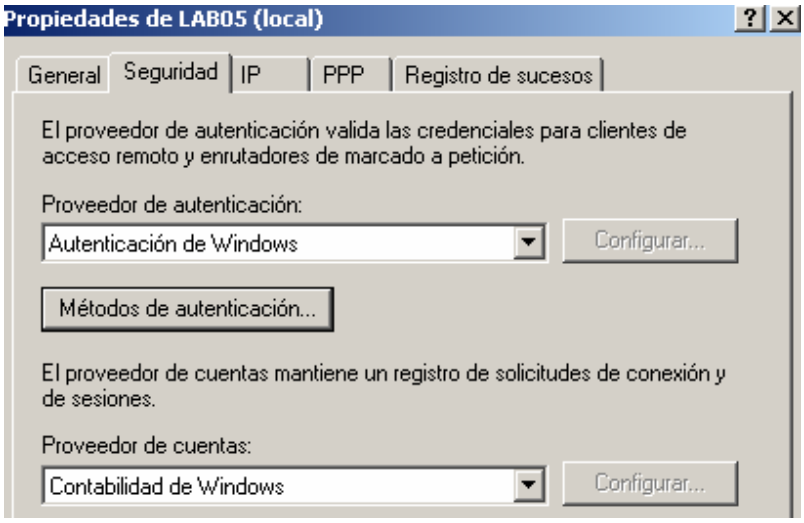


Figura 5.41 Propiedades de Servidor Local

Dar clic en el botón "Métodos de autenticación" para configurar el tipo de autenticación.

En la siguiente ventana (figura 5.42), se elige los metodos de autenticación: Autenticación cifrada de Microsoft versión 2 (MS-CHAP v2), Autenticación cifrada de Microsoft (MS-CHAP) y Autenticación cifrada (CHAP).

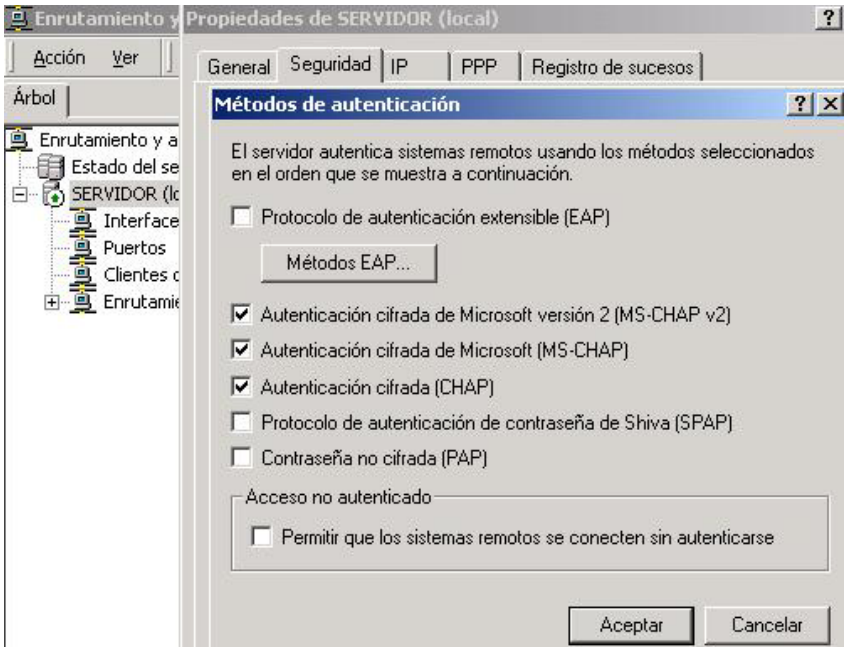


Figura 5.42 Métodos de autenticación

Normalmente, los clientes de Microsoft utilizan la autenticación MS-CHAP para proporcionar compatibilidad con tarjetas inteligentes. Los clientes que no son de Microsoft utilizan la autenticación CHAP, SPAP y PAP. En las conexiones PPTP cifradas, debe utilizar MS-CHAP como método de autenticación.

5.2.10 Pasos para la configuración del cliente VPN en Windows 2.000 Profesional

Los clientes de red privada virtual que se conectan al servidor de acceso remoto que ejecuta Windows 2000 Server pueden ser clientes Windows NT 4.0 o posteriores, o Windows 98 o posteriores. El cliente debe ser capaz de enviar paquetes TCP/IP al servidor de acceso remoto. Por lo tanto, se requiere un adaptador de red.

Utilizar el diagrama del laboratorio, y configurar el cliente en Windows 2.000 Profesional de la siguiente forma :

Paso 1 - Abrir "Inicio" → Configuración→

Acceso telefónico a redes

Paso 2 – En el asistente para conexión de red, elegir la opción "Conectar a una red privada a través de Internet"

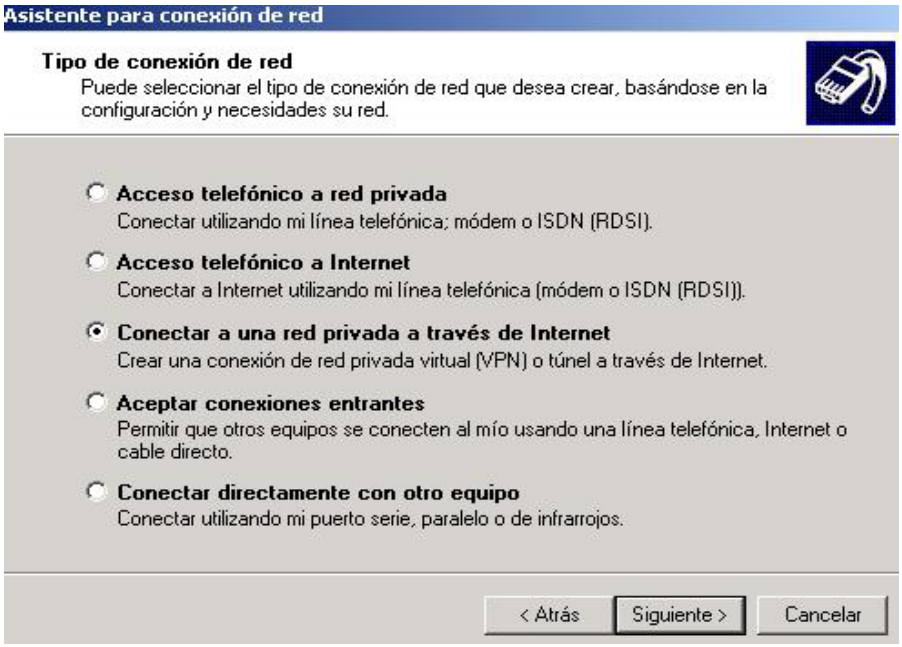


Figura 5.43 Tipo de conexión de red

En esta ventana (figura 5.15), digitar el nombre o IP del servidor VPN. Para la práctica, colocar la IP del servidor: 172.20.40.2

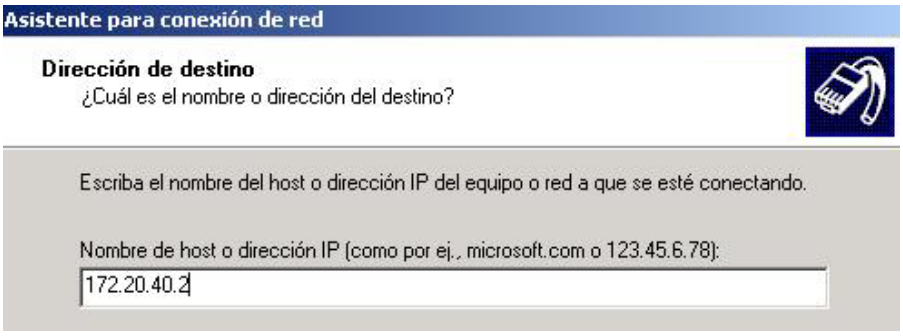


Figura 5.44 Dirección de destino

En la ventana "Finalización del asistente para conexión de red" (figura 5.16), escribir el nombre de la conexión VPN. Para la práctica, escribir: Conexión privada virtual.

Figura 5.45 Finalización del asistente para conexión de la red

Paso 3 - Comprobar la comunicación VPN entre el servidor y el usuario.

Abrir "Inicio" → Configuración→ Acceso telefónico a redes → Conexión privada virtual 

En la siguiente ventana (figura 5.17), escribir el nombre de usuario (Laboratorio) y la contraseña (practica).

Figura 5.46 Conectarse a conexión privada virtual

Dar clic en botón "Conectar" para establecer la conexión VPN.

6. CONCLUSIONES

Las redes virtuales V-LAN combinan mayores anchos de banda, facilidades de configuración y potencial de crecimiento. Otras Ventajas de las VLAN son:

- Una buena alternativa para transportar datos.
- Bajo el mismo equipo físico, diferentes agrupamientos lógicos.
- La interconexión e integración de servicios de información de diferentes sucursales alejadas geográficamente.

La forma de intercomunicación es segura y protegida de ataques externos.

Los servicios VPN permiten que los usuarios o las empresas se conecten de manera confiable a servidores remotos, sucursales u otras compañías sobre redes públicas y privadas, mientras mantienen una comunicación segura. En todos estos casos, la conexión segura se muestra ante el usuario como una comunicación de red privada, a pesar del hecho de que la comunicación ocurre sobre una red pública o privada. La tecnología VPN está diseñada para abordar asuntos relacionados con la actual tendencia de los negocios hacia operaciones globales cada vez mayores de telecomunicación y de amplia distribución, en donde los trabajadores deben poder conectarse a los recursos centrales y en donde los negocios deben poder comunicarse entre sí de manera eficiente.

LISTA DE TABLAS

Pág

LISTA DE FIGURAS

Pág

GLOSARIO

Administrador de red

Persona responsable del diseño, la configuración y la administración del funcionamiento diario de la red. El administrador de red se llama también administrador del sistema.

Autenticación

Proceso que se utiliza para comprobar que una entidad o un objeto es quien dice ser. Algunos ejemplos son la confirmación del origen y la integridad de la información, como la comprobación de una firma digital o de la identidad de un usuario o equipo.

Cifrado de clave pública

Método de cifrado que utiliza dos claves de cifrado relacionadas matemáticamente. Una se denomina clave privada y es confidencial. La otra

se denomina clave pública y se entrega gratuitamente a todos los posibles corresponsales. En una situación típica, un remitente utiliza la clave pública del destinatario para cifrar un mensaje. Sólo el destinatario tiene la clave privada correspondiente para descifrar el mensaje. La complejidad de esta relación entre la clave pública y la clave privada supone que, siempre que ambas tengan una longitud apropiada, resulta matemáticamente imposible determinar una a partir de la otra. El cifrado de clave pública se llama también cifrado asimétrico.

Clases de direcciones

Agrupaciones predefinidas de direcciones Internet. Cada clase define redes de un tamaño determinado. El intervalo de números que pueden asignarse al primer octeto de la dirección IP depende de la clase de dirección. Las redes de clase A (con valores de 1 a 126) son las mayores, con más de 16 millones de Hosts por red. Las redes de clase B (de 128 a 191) tienen hasta 65.534 Hosts por red y las redes de clase C (de 192 a 223) pueden tener hasta 254 Hosts por red.

Clave

Una clave puede contener subclaves y valores. En Seguridad de IP (IPSec), valor utilizado junto con un algoritmo para cifrar o descifrar datos. Para proporcionar mayor seguridad se pueden configurar los valores de las claves de seguridad de IP.

Conexiones de red

Componente que se puede utilizar para tener acceso a recursos y funciones de red, tanto si se encuentra físicamente en la ubicación de la red como si está en una ubicación remota. Mediante el uso de la carpeta Conexiones de red puede crear, configurar, almacenar y supervisar conexiones.

Conmutación de paquetes

Tecnología utilizada para desglosar los datos en paquetes y, después, enviarlos a través de una red. Cada paquete tiene un encabezado que contiene su origen y destino, un número de secuencia para volver a ensamblar la información, un bloque de contenido de datos y un código de comprobación de errores. Los paquetes de datos pueden tomar rutas diferentes para llegar a su destino, donde la información original se vuelve a ensamblar cuando llegan los

paquetes. El estándar internacional para las redes de conmutación de paquetes es X.25.

Contraseña

Medida de seguridad para restringir los nombres de inicio de sesión a cuentas de usuario y el acceso a los sistemas y recursos. Una contraseña es una cadena de caracteres que hay que suministrar para obtener la autorización para un acceso o un nombre de inicio de sesión. Una contraseña puede estar formada por letras, números y símbolos, y distingue mayúsculas de minúsculas.

Contraseña cifrada

Contraseña codificada. Las contraseñas cifradas son más seguras que las de texto simple, que pueden ser capturadas por piratas de la red.

Criptografía

Procesos, ciencia y arte de conservar mensajes y datos de forma segura. La criptografía se utiliza para habilitar y asegurar la confidencialidad, la integridad

de los datos y la autenticación (origen de datos y entidad), y para evitar el rechazo.

Criptografía de claves públicas

Método de criptografía que utiliza dos claves diferentes: una clave pública para cifrar datos y otra privada para descifrarlos.

Difusión

Dirección que tiene como destino todos los Hosts de un segmento de red determinado.

Dirección IP

Dirección de 32 bits utilizada para identificar un nodo en un conjunto de redes IP. Cada nodo de un conjunto de redes IP debe tener asignada una dirección IP única, que está formada por el identificador de red más un identificador de Host único. Normalmente, esta dirección se representa con el valor decimal de cada octeto separado por un punto (por ejemplo, 192.168.7.27).

Dominio

Grupo de equipos que forman parte de una red y comparten una base de datos de directorio común. Un dominio se administra como una unidad con reglas y procedimientos comunes. Cada dominio tiene un nombre único.

Enrutador

Hardware que contribuye a que las redes de área local y de área extensa (LAN y WAN) dispongan de las capacidades de interacción y conexión, y puedan vincular LAN con topologías de red diferentes (como Ethernet y Token Ring). Los enrutadores asocian los encabezados de paquete a un segmento de LAN y eligen la mejor ruta para el paquete, optimizando el rendimiento de la red.

Los enrutadores son necesarios para que los equipos de redes físicas diferentes se comuniquen entre sí. Los enrutadores mantienen un mapa de las redes físicas en una red interna y reenvían los datos recibidos desde una red física a otras redes físicas.

Enrutamiento

Proceso que consiste en reenviar un paquete a través de redes interconectadas desde un Host de origen a un Host de destino.

Equipo de comunicaciones de datos (DCE)

Uno de los dos tipos de hardware conectados mediante una conexión serie RS-232-C; el otro es un dispositivo del tipo Equipo terminal de datos (DTE, Data Terminal Equipment). Un DCE es un dispositivo intermedio que normalmente transforma la entrada de un DTE antes de enviarla a su destinatario. Por ejemplo, un módem es un DCE que modula datos de una microcomputadora (DTE) y los envía a través de una conexión telefónica.

Equipo terminal de datos (DTE)

En el estándar de hardware RS-232-C, cualquier dispositivo, como un cliente o un servidor de acceso remoto, que pueda transmitir información en forma digital a través de un cable o una línea de comunicación.

Escalabilidad

Medida de la eficacia del crecimiento de un equipo, servicio o aplicación para satisfacer las exigencias de aumento del rendimiento.

Filtro

En IPSec, especificación de tráfico IP que proporciona la capacidad de desencadenar negociaciones de seguridad para una comunicación basada en el origen, el destino y el tipo de tráfico IP.

Herramientas de administración y supervisión

Componentes de software que incluyen utilidades para la administración y supervisión de redes, así como servicios que admiten llamadas de clientes y permiten la actualización de sus libretas de teléfonos.

Host

Equipo donde se ejecuta un servicio o programa de servidor que utilizan clientes de red o remotos.

Intercambio de paquetes entre redes (IPX)

Protocolo de red de NetWare encargado de dirigir y enrutar los paquetes dentro de las redes de área local (LAN) y entre ellas. IPX no garantiza que un mensaje llegue completo (sin pérdida de paquetes).

Interfaz de usuario extendida de NetBIOS (NetBEUI)

Protocolo de red de Conexiones de red de Microsoft. Normalmente se utiliza en redes de área local (LAN) pequeñas, características de un departamento, de 1 a 200 clientes. El único método de enrutamiento que puede utilizar es enrutamiento de origen Token Ring. Es la implementación de Microsoft del estándar NetBIOS.

Internet

Dos o más segmentos de red conectados mediante enrutadores. Red mundial de equipos.

L2TP (Protocolo de túnel de nivel 2)

Protocolo de túnel de Internet normalizado. A diferencia del Protocolo de túnel punto a punto (PPTP, Point-to-Point Tunneling Protocol), L2TP (Layer 2 Tunneling Protocol) no requiere conectividad IP entre la estación de trabajo de cliente y el servidor. Sólo requiere que el túnel proporcione conectividad punto a punto orientada a paquetes. Este protocolo se puede utilizar en medios como ATM, Frame Relay y X.25. L2TP ofrece la misma funcionalidad que PPTP. Basado en las especificaciones Layer 2 Forwarding 2 (L2F) y PPTP, L2TP permite a los clientes establecer túneles entre las redes que intervienen.

Máscara de subred

Valor de 32 bits que permite al destinatario de paquetes IP diferenciar la parte del identificador de la red y la del identificador del Host en la dirección IP. Por lo general, las máscaras de subred utilizan el formato 255.x.x.x.

Módem (modulador/desmodulador)

Dispositivo que permite transmitir y recibir información en un equipo a través de una línea telefónica. El módem transmisor traduce los datos digitales de los equipos a señales analógicas que se pueden transmitir a través de la línea telefónica. El módem de destino vuelve a traducir las señales analógicas recibidas a formato digital.

Nombre de dominio

Nombre que un administrador asigna a un grupo de equipos conectados en red que comparten un directorio común. Como parte de la estructura de nomenclatura del Sistema de nombres de dominio (DNS), los nombres de dominio constan de una secuencia de etiquetas de nombre separadas por puntos.

Nombre de Host

Nombre DNS de un dispositivo de una red. Estos nombres se utilizan para buscar equipos en la red. Para buscar otro equipo, el nombre de host debe figurar en el archivo Hosts o ser conocido por un servidor DNS.

Opción DHCP

Parámetros de configuración de direcciones que un servidor DHCP asigna a los clientes. La mayor parte de las opciones de DHCP están predefinidas, en función de parámetros opcionales definidos en el documento Solicitud de comentarios (RFC, Request For Comments).

Ping

Utilidad que comprueba las conexiones con uno o varios Hosts remotos. El comando ping utiliza los paquetes de solicitud de eco y de respuesta de eco ICMP para determinar si un sistema IP específico funciona en una red. Ping resulta útil para diagnosticar los errores en redes o enrutadores IP.

Protocolo de control de transporte/Protocolo de Internet (TCP/IP)

Conjunto de protocolos de red muy utilizados en Internet que permiten la comunicación entre redes interconectadas formadas por equipos con distintas arquitecturas de hardware y sistemas operativos. TCP/IP incluye estándares para la comunicación entre equipos y convenciones para conectar redes y enrutar las transmisiones.

Protocolo de datagramas de usuario (UDP)

Complemento de TCP que ofrece un servicio de datagramas sin conexión que no garantiza la entrega o la secuencia correcta de los paquetes entregados (de forma similar a IP).

Protocolo de Internet (IP)

Protocolo de enrutamiento del conjunto de protocolos TCP/IP responsable de la asignación de direcciones IP, el enrutamiento y la fragmentación y ensamblaje de paquetes IP.

Protocolo punto a punto (PPP, Point-to-Point Protocol)

Conjunto de protocolos estándar para el uso de vínculos punto a punto en el transporte de datagramas multiprotocolo.

Proxy WINS

Equipo que escucha las difusiones de consultas de nombres y responde cuando éstos no se encuentran en la subred local. El proxy se comunica con un servidor WINS para resolver los nombres y luego los almacena localmente durante un intervalo de tiempo determinado.

Puerta de enlace

Dispositivo conectado a múltiples redes TCP/IP físicas y capaz de enrutar o transportar paquetes IP de unas a otras. Una puerta de enlace o gateway traduce los distintos protocolos de transporte o formatos de datos (por ejemplo IPX e IP) y, generalmente, se agrega a las redes por su capacidad de traducción.

Puerto

Punto de conexión del equipo al que puede conectar dispositivos que reciben y envían datos. Por ejemplo, normalmente se conecta la impresora a un puerto paralelo (denominado también puerto LPT) y un módem suele conectarse a un puerto serie (denominado también puerto COM).

Red

Grupo de equipos y otros dispositivos, como impresoras y escáneres, conectados mediante un vínculo de comunicaciones, lo que permite la interacción de todos los dispositivos entre sí. Las redes pueden ser grandes o pequeñas, y estar conectadas siempre mediante cables o temporalmente mediante líneas telefónicas o transmisiones inalámbricas. La red más grande es Internet, que es un grupo mundial de redes.

Red de área local (LAN)

Red de comunicaciones que conecta un grupo de equipos, impresoras y otros dispositivos que se encuentran en un área relativamente limitada (por ejemplo, un edificio). Una LAN permite a los dispositivos conectados interactuar con otros dispositivos de la red.

Rutas estáticas

Rutas de la tabla de enrutamiento que son permanentes. Las rutas estáticas son configuradas manualmente por un administrador de la red. Sólo cambian si el administrador de la red las cambia. Si el protocolo de enrutamiento se configura para admitir rutas autoestáticas (rutas estáticas agregadas automáticamente), el enrutador puede emitir una solicitud a un protocolo para obtener una actualización de la información de enrutamiento en una interfaz específica. Después, los resultados de esta actualización se convierten y mantienen como rutas estáticas.

Seguridad

En una red, protección de un sistema informático y sus datos contra daños o pérdidas, que se implementa especialmente para que sólo los usuarios autorizados puedan tener acceso a los archivos compartidos.

Seguridad de Protocolo de Internet (IPSec)

Conjunto de protocolos y servicios de protección estándares del sector basados en criptografía. IPSec protege todos los protocolos del conjunto de protocolos TCP/IP y comunicaciones de Internet mediante L2TP.

Servicio de usuario de acceso telefónico de autenticación remota (RADIUS)

Protocolo de autenticación de seguridad con clientes y servidores, muy utilizado por los proveedores de servicios Internet (ISP) en servidores remotos de sistemas operativos que no son Windows. RADIUS es el método más conocido de autenticación y autorización de usuarios de acceso telefónico y redes de túnel.

Topología

Relación entre un conjunto de componentes de red.

Túnel

Conexión lógica a través de la que se encapsulan los datos. Normalmente, los datos se encapsulan y se cifran, y el túnel es un vínculo seguro y privado entre un usuario remoto o un Host y una red privada.

RESUMEN

Las LANs virtuales (V-LANs) son agrupaciones de estaciones, definidas por software, que se comunican entre sí como si estuvieran conectadas al mismo concentrador, aunque se encuentren situadas en segmentos diferentes de una red de edificio o de campus. Es decir, la red virtual es la tecnología que permite separar la visión lógica de la red de su estructura física. Una de las ventajas para implementar V-LAN es por que proporcionan seguridad, protección de la inversión, movilidad y conectividad.

Una Red Privada Virtual (VPN) es una forma de compartir y transmitir información entre un círculo cerrado de usuarios que están situados en diferentes localizaciones, mediante un proceso de comunicación cifrado o encapsulado que trasfiere datos desde un punto hacia otro de manera segura, y los datos que se transfieren pasan a través de una red abierta, insegura y enrutada. Además los servicios de VPN incluyen autentificación, integridad de datos y encriptación. Por lo tanto una VPN es un túnel encriptado y seguro. En cuanto a seguridad, IPSec provee servicios de privacidad y autentificación en túneles sobre redes no seguras.

Se elaboraron y documentaron las siguientes practicas de V-LAN: práctica de V-LAN por puerto con un Switch, práctica de V-LAN por puerto con dos Switch

por medio de trunk, práctica de comunicación entre V-LAN con un Switch por medio de un Router, práctica de comunicación entre V-LAN con dos Switch por medio de un Router.

Se desarrollaron las siguientes practicas de VPN: práctica de PPP como funcionamiento básico de VPN en el Router y práctica de configuración de VPN en Windows 2000 Server

RECOMENDACIONES

Para futuras investigaciones con respecto a esta monografía, con el fin de mejorarla y/o profundizar en algunos aspectos:

- La practica de Comunicación entre V-LAN con un Switch por medio de un Router se puede configurar o implementar un servicio (Ej. http, Web, correo electrónico, etc.) en un servidor y permitir que a través del Router, las V-LAN puedan acceder a estos servicios.

- La práctica de VPN se puede implementar a través de Internet mediante una conexión de acceso remoto, aplicando un servidor Radius,.

- La práctica de PPP, se puede implementar comunicando dos redes LAN (una en cada lado de cada Router) aplicando autenticación de usuarios por protocolo de autenticación CHAP.

- En la práctica de VPN, se puede implementar una comunicación VPN entre dos redes, donde la red 1 este conectada a la tarjeta de red 1 y la red 2 este conectada a la tarjeta 2.

BIBLIOGRAFÍA

LIBROS

Redes Privadas Virtuales (VPN)

- Cisco Systems, inc., Guía del primer año – segunda edición. Pearson Education, 2.001
- Cisco Systems, inc., Guía del segundo año – segunda edición. Pearson Education, 2.001
- Steven Brown, Implementación de redes privadas virtuales (RPV), Mc Graw Hill, 2000
- Martin Murhammer, et alt. , "A Comprehensive Guide to Virtual Private Networks, Volume I", IBM Redbooks, 1.998

lC. Scott, P. Wolfe, M. Erwin , "Virtual Private Networks", O'Reilly, 1.998

Criptografía y Seguridad

- W. Stallings, “Cryptography and Network Security”, Prentice Hall, 1.999

DIRECCIONES DE INTERNET

Redes

- www.alojamiento24h.com/page18.html
- www.gsyc.inf.uc3m.es/~jjmunoz/lro/9798/copia/%257Ecalonso
- www.pagina.de/inforedes
- www.reinicianetwork.com/internet.htm
- http://alonso_m.tripod.com/bookmark.htm
- http://www.helpagora.com/_shd/iniciohelpnewslistado.asp

Redes Virtuales a través de enlaces LAN (VLAN)

- Creating and Maintaining VLANs, www.cisco.com/univercd/cc/td/doc/product/lan/c2900xl/29_35xu/scg/kivlan.htm
- 3com Transcend VLANs, www.3com.com/nsc/200375.html
- Cisco About VLAN, www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/sw_ntman/vlandir/vdir1gsg/overvw.htm
- Understanding VLANs, www.cisco.com/univercd/cc/td/doc/product/rtrmgmt/sw_ntman/vlandir/vdir1gsg/overvw.pdf
- www.itlp.edu.mx/publica/revistas/revista_isc/anteriores/jun99/vlan.html
- www.itlp.edu.mx/publica/revistas/revista_isc/actual/vlan.htm
- www.ciscoredaccionvirtual.com/redaccion/glosario/default.asp?letra=V
- www.cnice.mecd.es/tecnologica/experto/interconexion/index.htm
- http://cum.unex.es/profesores/hdezcham/software/Software%20Prácticas/VLANs1.pdf
- http://www.consulintel.es/Html/Tutoriales/Articulos/vlan.html
- http://www.angelfire.com/al4/vlan/LABORATO.htm
- www.itlp.edu.mx/publica/revistas/revista_isc/actual/vlan.htm
- http://www.infortisa.com/ftp/produ/220037.htm

- http://www.longshine.es/Switches/sw2400.htm
- http://www.sistecon.com.mx/gigabit_cobre.htm
- http://www.optimumdata.com/pdf/cisco/es/switches/3000.pdf
- http://www.abcnet.es/notasinf/478-1412.html
- http://www.arrays.com.ar/productos/cisco/ciscoSwitch2900-100.pdf
- http://docs.sun.com/source/816-4620-10/Vendor2.html#pgfId-1072852
- support.ap.dell.com/docs/NETWORK/9195P/sp/nw_team.htm

Dispositivos de VLAN

- http://www.3com.com

Redes Privadas Virtuales (VPN)

- lro9798/vpn.htm
- lro9798/ungla.dit.upm.es/~pepe/ec/05f-vpn.pdf
- http://www.conecsion.es/soporte.htm
- http://www.linuxware.com.mx/vpn.php

- http://www.conecsion.es/sat/draytek/vpns/pasoapaovpn_archivos/vpn1.htm
- http://www.conecsion.es/sat/draytek/vpns/pasoapaovpns.htm
- http://infoacceso.upv.es/accpub/winxp/WinXP.htm
- http://www.cisco.com/en/US/netsol/ns110/ns170/ns171/ns27/networking_solutions_package.html
- www.cisco.com/en/US/netsol/ns110/ns170/net_solution_home.html
- http://ttt.upv.es/asegur/vpn.htm
- http://corporativo.andinanet.net/new/pages/prod.html
- http://www.cisco.com/global/LA/LATAM/sne/bancos.shtml
- http://www.microsoft.com/spain/technet/implantacion/cap17.asp
- http://www.ecocomputer.com/empresas/vpn/default.php

Dispositivos de VPN

- http://www.netmedia.info/informationweek/articulos.php?id_sec=46&id_art=972
- www.cisco.com/go/offices
- http://www.cisco.com/cgi-bin/order/order_root.pl
- http://www.cisco.com/warp/public/cc/si/casi/ca6000/
- http://www.cisco.com/warp/public/cc/rt/7600sr/index.shtml
- http://www.cisco.com/warp/public/779/largeent/learn/technologies/vpns.html

- http://www.cisco.com/warp/public/779/largeent/issues/security
- www.cisco.com/warp/public/cc/pd/rt/7100/prodlit/vpnsp_pg.ppt
- http://www.cisco.com/warp/public/cc/pd/si/casi/ca6000/ps4221
- http://www.cisco.com/warp/public/779/largeent/learn/technologies/vpn/ra_vpn.html
- http://www.cisco.com/warp/public/779/largeent/learn/technologies/vpn/site2site.html
- http://www.cisco.com/warp/public/cc/pd/si/casi/ca6000/ps4221/
- http://www.cisco.com/warp/public/cc/pd/fw/sqfw500/
- http://www.cisco.com/warp/public/cc/pd/hb/vp3000/
- www.cisco.com/warp/public/cc/pd/rt/7100/prodlit/iovpn_ds.pdf
- http://www.cisco.com/warp/public/cc/pd/rt/7600osr/index.shtml
- www.cisco.com/warp/public/cc/pd/rt/7100/prodlit/vpnss_ds.htm
- www.cisco.com/warp/public/cc/pd/rt/7100/prodlit/1019_pp.htm
- http://www.perle.com/products/data_sheets/access_servers/BR_833AS_SP.pdf
- http://www.helpagora.com/_shd/helpnewsnoticia.asp?id=129
- http://www.cisco.com/GO/VPN

IPSec

- www.openbsd.org/faq/es/faq13.html
- www.openbsd.org/faq/es/faq13.html
- seguridad.diatel.upm.es/IPv6eIPSec.htm
- www.consecri.com.ar/pdf/Consecri%2026-09-01/Sal%F3n%20General/Exposiciones/09-Protocolo%20IPSEC.pdf
- seguridad.internet2.ulsa.mx/congresos/2001/cudi2/tutorial_ipsec.pdf
- www-mat.upc.es/~jforne/ipsec.pdf
- www.consecri.com.ar/pdf/Consecri%2026-09-01/Sal%F3n%20Multimedia/Exposiciones/19-soporte%20seguridad%20sitios%20web.pdf
- http://www.acis.org.co/Paginas/noticias/seguridad2.html
- http://www.conecsion.es/sat/draytek/vpns/pasoapaovpn_archivos/IPSec%20Tunnel.htm

Criptografía y Seguridad

- www.sun.com/security/skip